



Paraben's Shuttle Pro 1.3.0 Release Notes

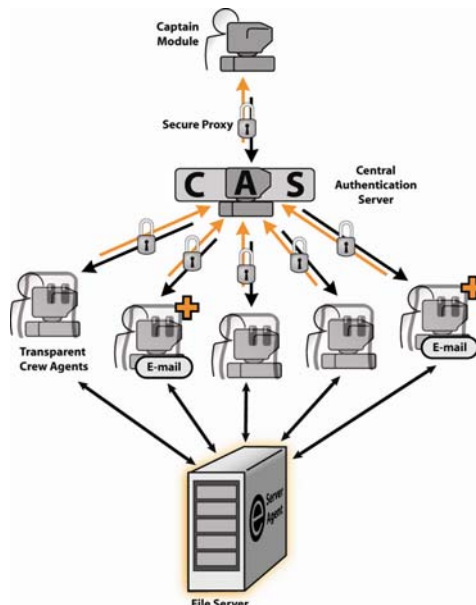
Welcome to Paraben's Shuttle Pro 1.3.0!

Paraben's Shuttle Pro (PSPro) is an enterprise investigation tool that provides cutting edge deployable forensic solutions. It is the ideal network incident response tool and the perfect live forensic solution for examiners who deal with incident response.

Shuttle Pro has immense capabilities, including the ability to view, acquire, and search client data in an enterprise without detection and using forensically sound methods, so you can effectively respond to incidents, collect crucial evidence, and produce detailed reports.

Shuttle Pro is comprised of four primary modules, each of which completes unique tasks and collaborates with other modules to provide the robust functionality available with Shuttle. Typically, the modules are located on different computers but they can all be located on a single machine. The following modules make up P2 Shuttle:

- P2S Crew Agent
- P2S Captain
- P2S Central Authentication Server
- P2S Proxy



What's new in Paraben's Shuttle Pro 1.3.0

- Agent auto-update feature for quick updating of all Agents to a newer version.
- Parsing of email databases of multiple format without acquisition:
 - Microsoft Exchange 5.0, 5.5, 2000, 2003 SP1, 2007 (EDB)
 - Lotus Notes 4.0, 5.0, 6.0, 7.0, 8.0
 - Novell GroupWise
 - Microsoft Outlook (PST)
 - Microsoft Outlook Express (EML)
 - E-mail Examiner (EMX)
 - AOL
 - The Bat! (3.x and higher)
 - Thunderbird
 - Windows Mail
 - Eudora
- Parsing of chat databases of multiple format without acquisition:
 - Yahoo!
 - Skype
 - ICQ
 - Miranda
 - Hello (including thumbnails)
 - Trillian
- Parsing of Internet Explorer and Mozilla Firefox browser history without acquisition.
- Improved performance and stability.
- And much more!

This document provides you with a list of all Shuttle Pro key features and a full list of key changes in version 1.3.0.



Shuttle Pro 1.3.0 New Features

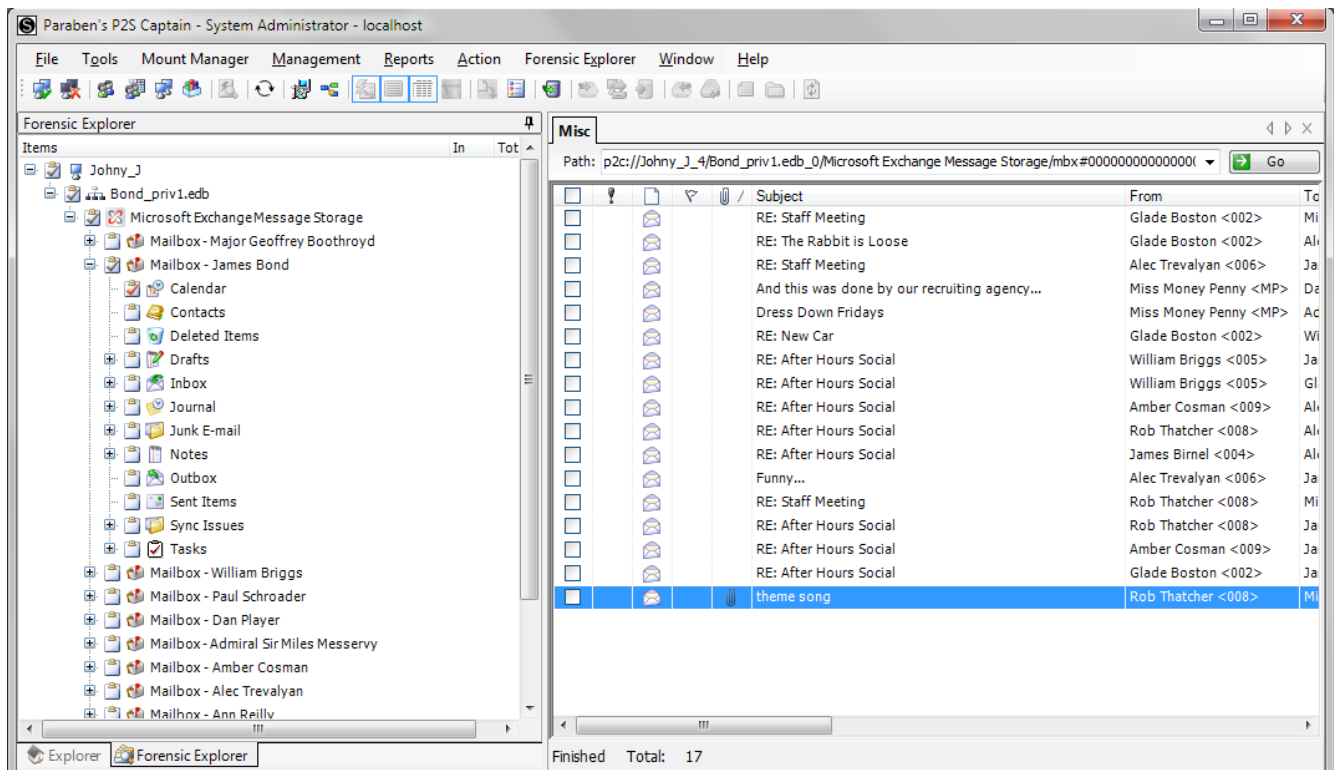
The following features have been added to the Paraben's Shuttle 1.3.0 with this release:

General Changes:

- Better memory management –several leaks fixed when working with big databases.
- Performance and operation bugs were fixed.
- Possible problems when working on computers with different configurations were detected and fixed.
- GUI was improved for better usability.

New Features:

- **Analysis of email databases of different formats on the Agent computer:**
 - Viewing structure and contents of parsed mail stores including deleted messages, Calendar and Contacts entries.



Paraben's Shuttle Pro 1.3.0 Release notes

- Viewing message header and message body in different formats (HTML, RTF, Plain text, etc.)

The screenshot displays the Paraben's Shuttle Pro 1.3.0 interface. At the top, a window titled "Misc" shows a file path: p2c://Johny_J_4/Bond_priv1.edb_0/Microsoft Exchange Message Storage/mbx#0000000000000001/mbx#0000000000000001:fld#00. Below the path is a "Go" button. A table lists email messages:

	Subject	From	To	Created
<input type="checkbox"/>	RE: After Hours Social	Amber Cosman <009>	James Bond <007@MI6.UK>	13.04
<input type="checkbox"/>	RE: After Hours Social	Glade Boston <002>	James Bond <007@MI6.U>	13.04
<input type="checkbox"/>	theme song	Rob Thatcher <008>	Miss Money Penny <MP@>	14.04

Below the table, it says "Finished Total: 17". The main area is titled "E-mail Data" and shows the details for the selected "theme song" message:

theme song
"Rob Thatcher" <008>
To: Miss Money Penny <MP@MI6.UK.GOV>, Admiral Sir Miles Messervy <M@MI6.UK.GOV>, Alec Trevelyan <006@MI6.UK.GOV>, Amber Cosman

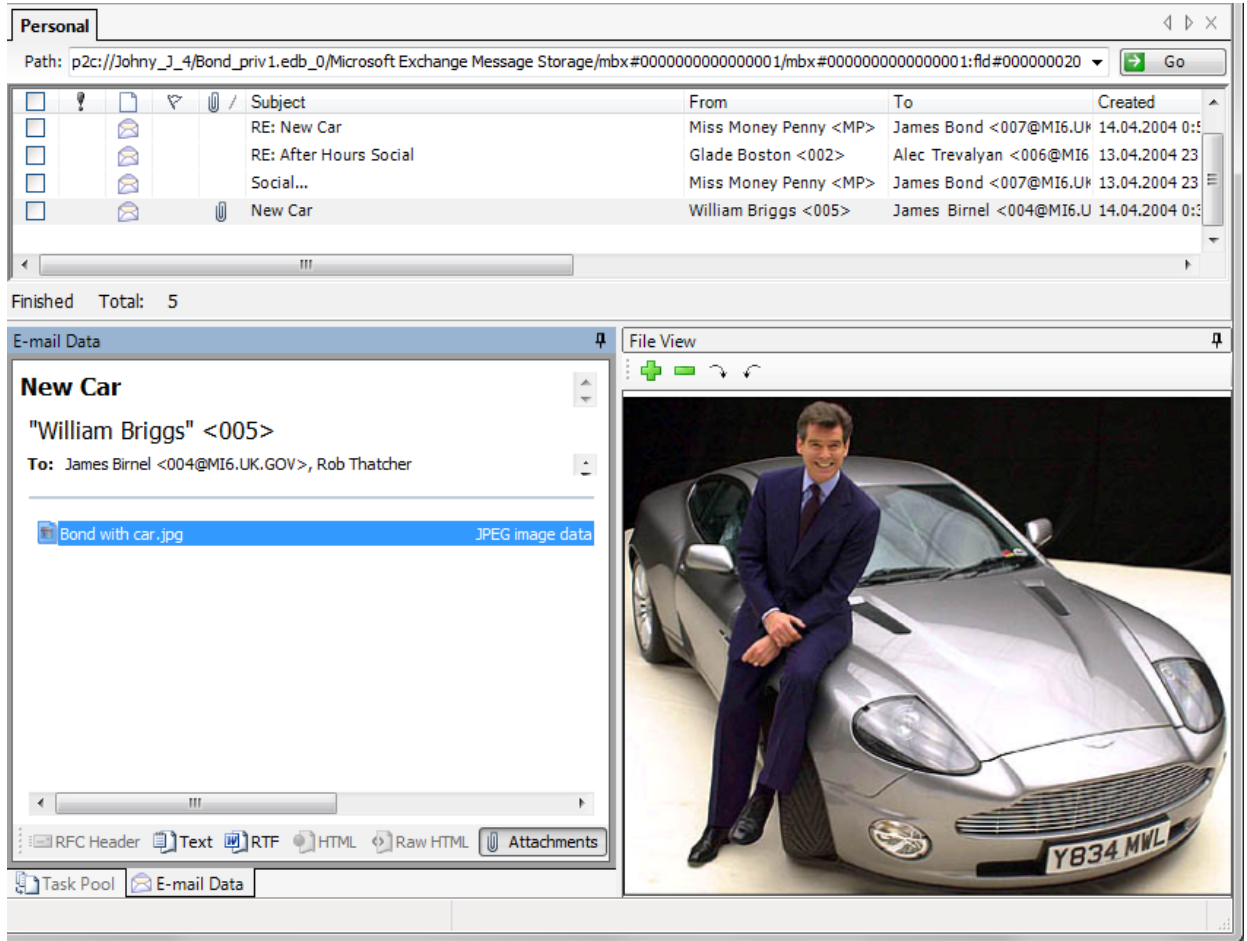
Wouldnt it be cool if we had a theme song that played while we were working. Check this one out.
-008

From: Miss Money Penny
Sent: Tuesday, April 13, 2004 2:46 PM
To: Admiral Sir Miles Messervy; Alec Trevelyan; Amber Cosman; Ann Reilly; Glade Boston; James Bond; Major Geoffrey Boothroyd; Miss Money Penny; Paul Schroader; Rob Thatcher; William Briggs
Subject: Dress Down Fridays

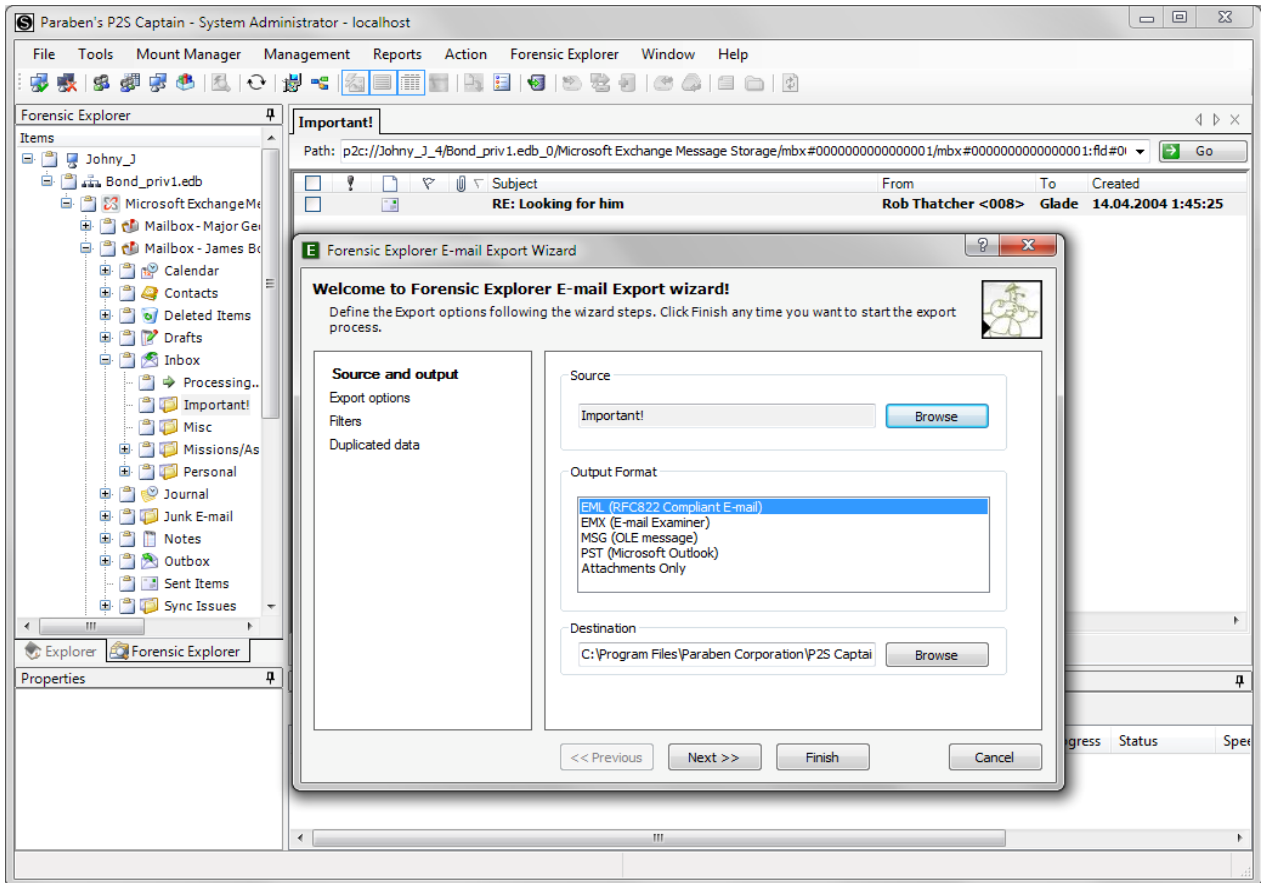
To: Staff

At the bottom, a toolbar contains icons for "RFC Header", "Text", "RTF", "HTML", "Raw HTML", and "Attachments". The "Text" icon is highlighted with an orange box. Below the toolbar are tabs for "Task Pool" and "E-mail Data".

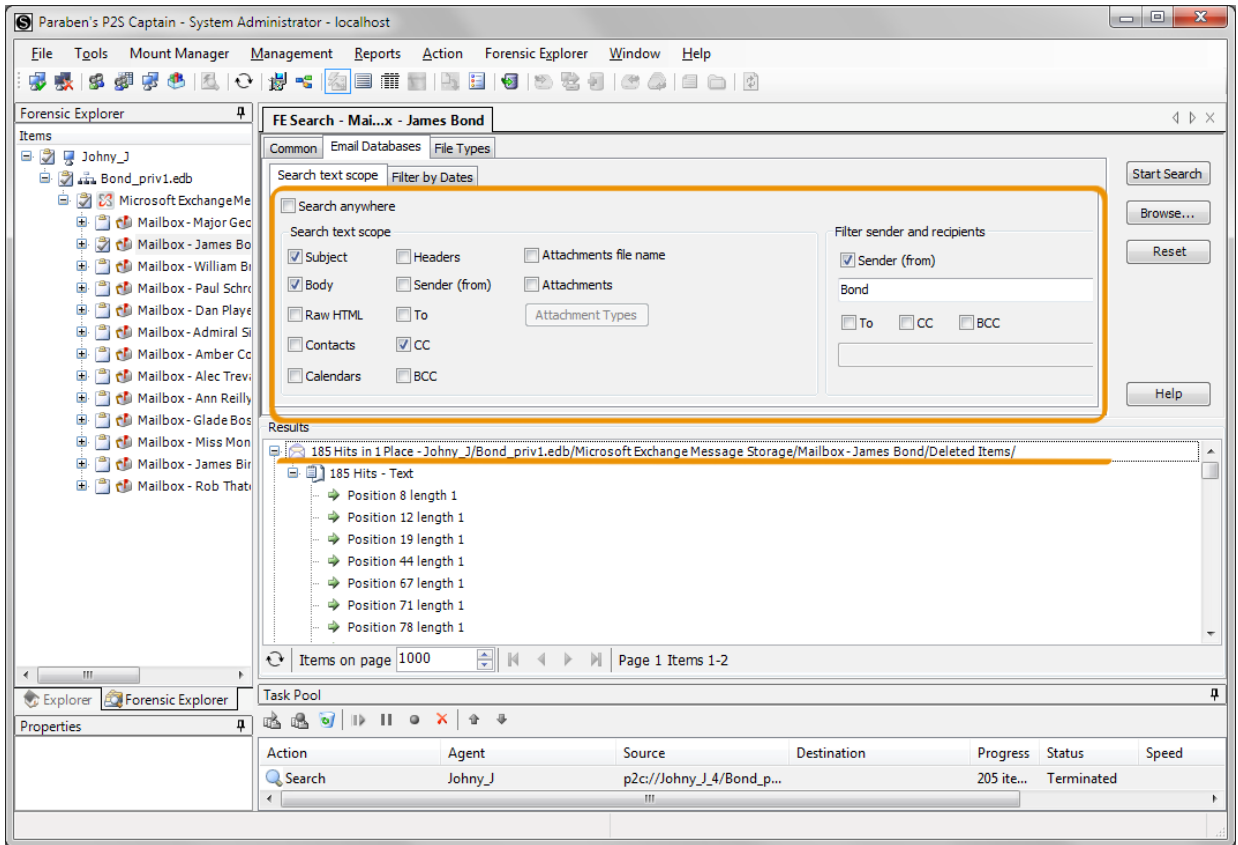
- o Viewing attachments in a special File viewer.



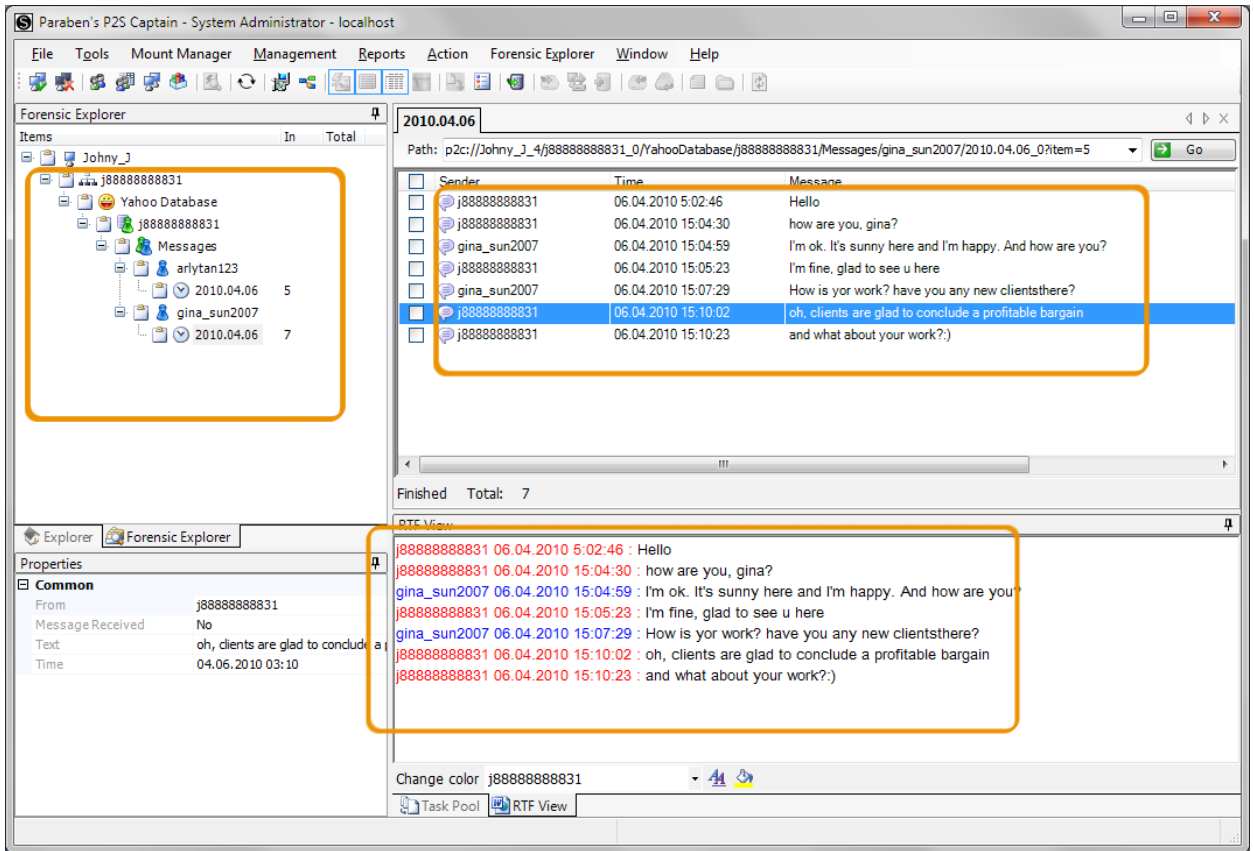
- Exporting data to several formats.



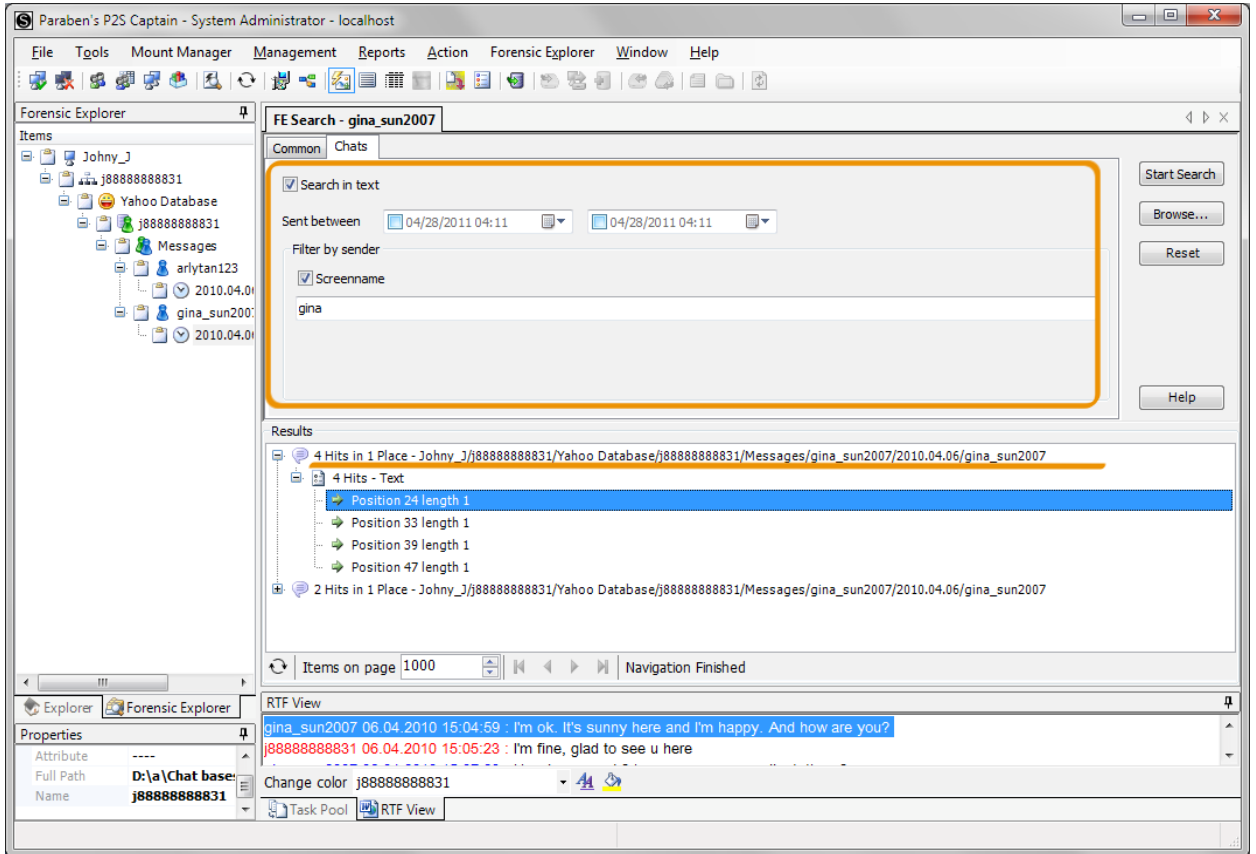
- Multi-parameter search in email database.



- **Analysis of chat databases of different formats on the Agent computer:**
 - Viewing parsed chat database structure and conversations.

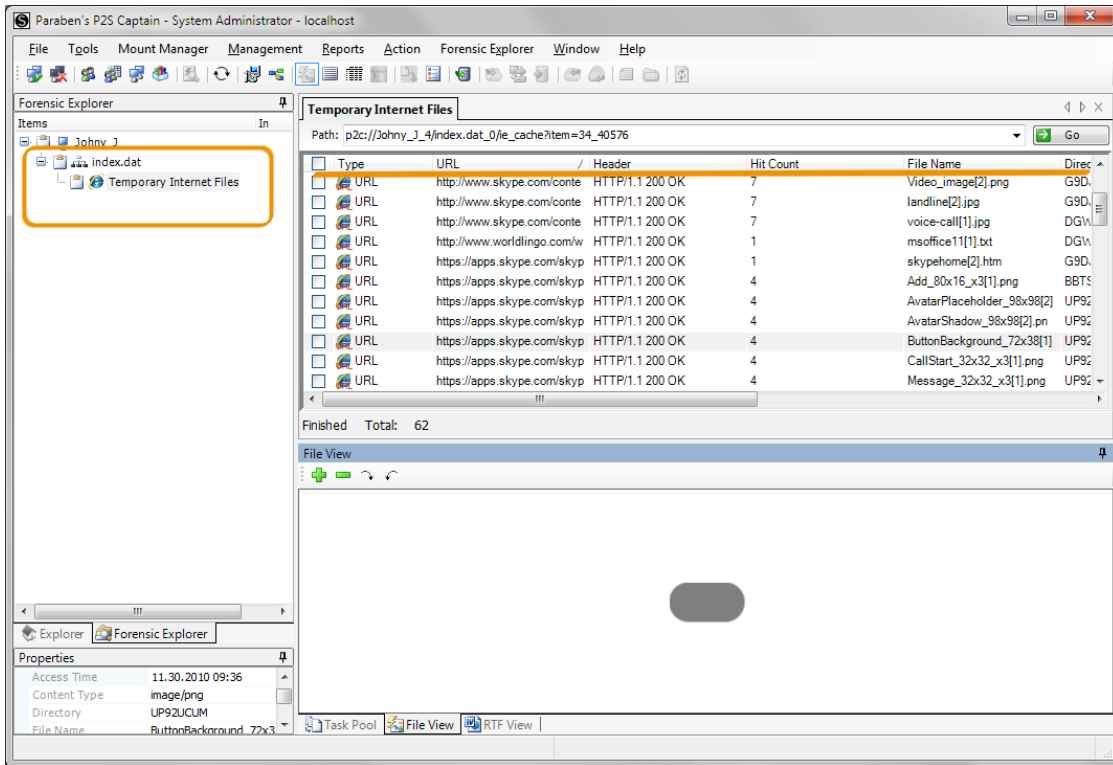


- Multi-parameter search in chat database.

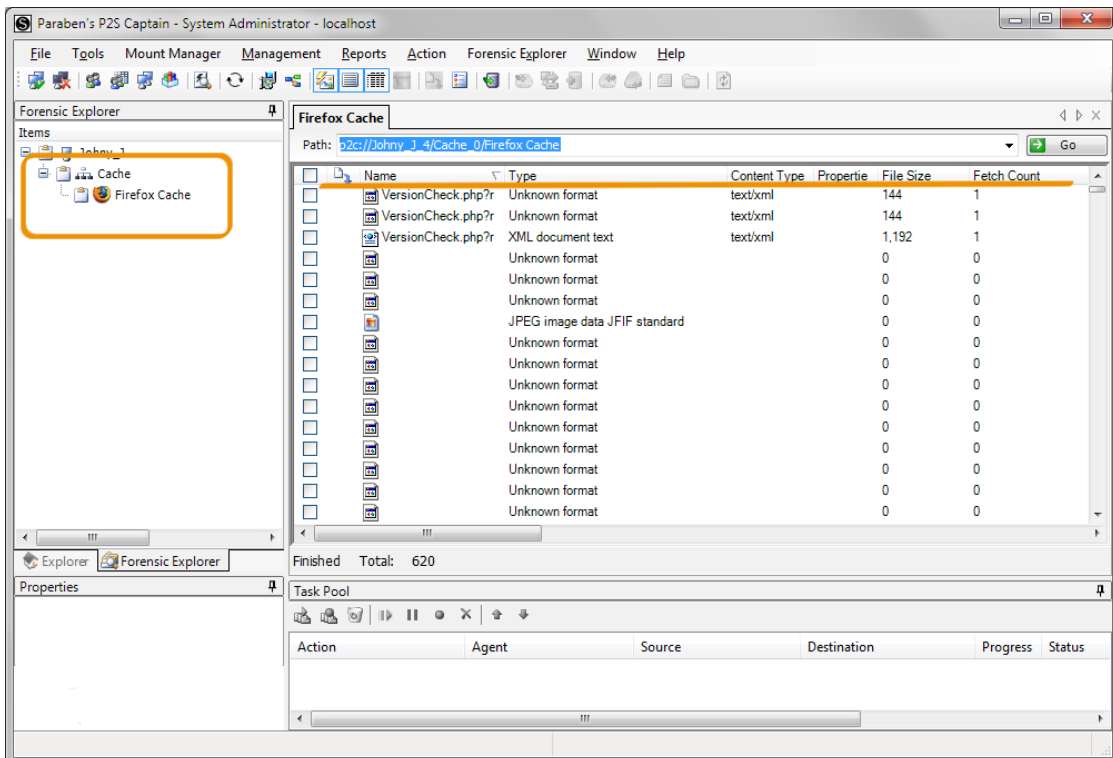


- **Analysis of Internet browser data on the Agent computer:**

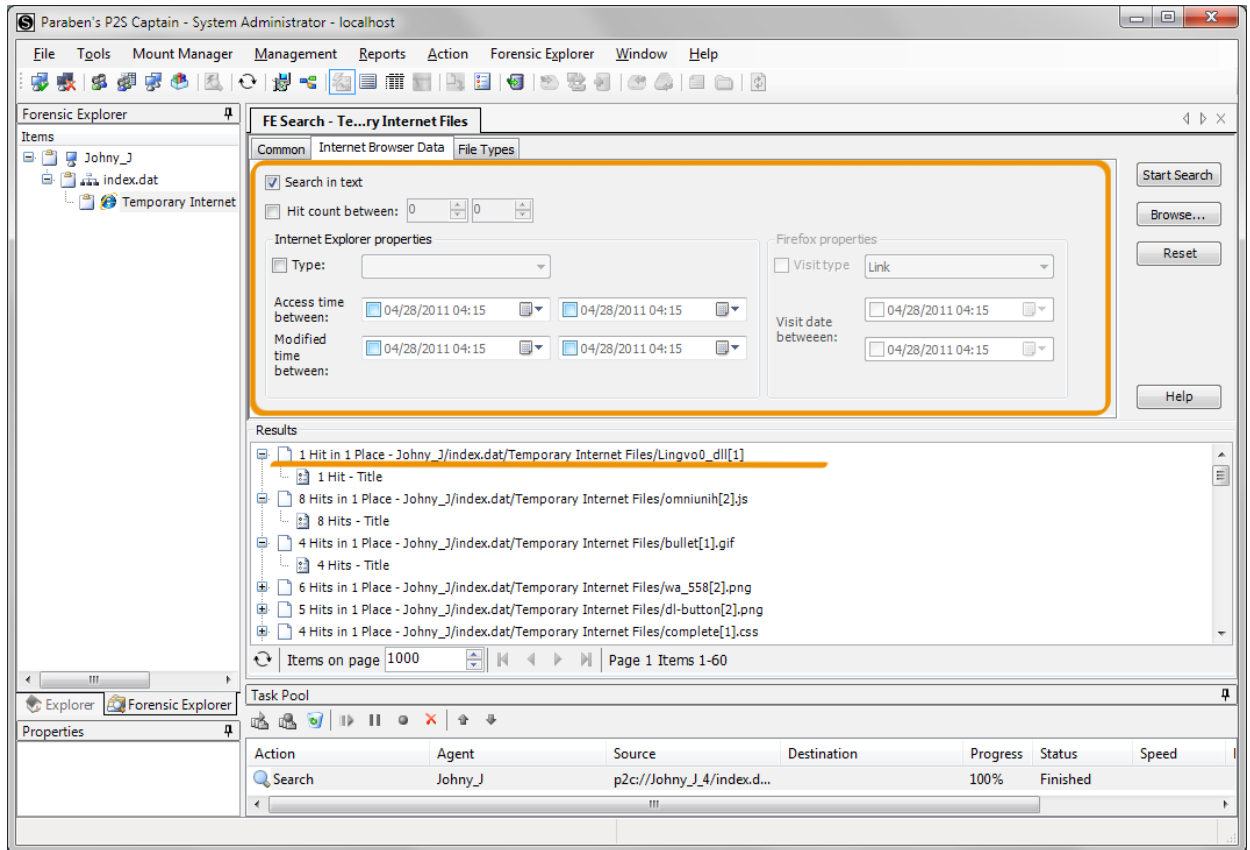
- Viewing history, cookies, and temporary Internet files for Internet Explorer.



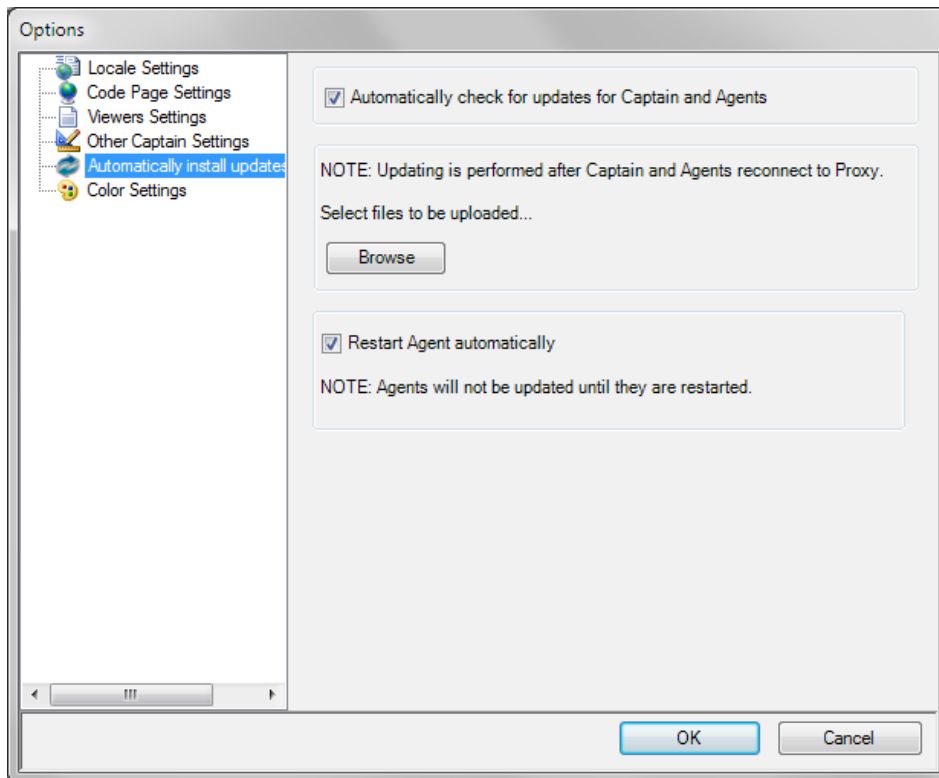
- Viewing history and cache data for Mozilla Firefox.



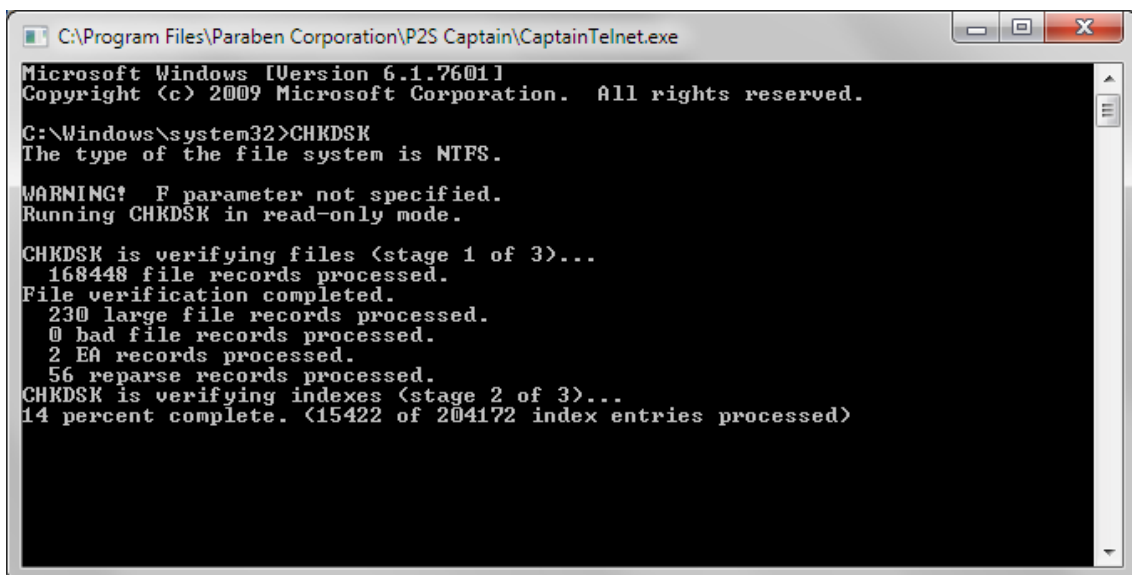
- Multi-parameter search in Internet Browser data.



- **Agent auto-update allows you to automatically update Agent version on multiple version after updating Proxy version.**



- **Telnet allows to manage Agent remotely using command-line interface.**



Paraben's Shuttle Pro Key Features

Paraben's Shuttle Pro 1.3.0 has the following key features:

General features:

- Multi-machine Agent installation.
- Agent safe mode for being completely unnoticeable on the investigated computer.
- Encrypted connection for data communication between all parts of P2 Shuttle.
- Back-end Firebird database for support of massive amounts of data on Server.
- Multi-threading and task scheduling capabilities to process more data in less time.
- Full Windows 7 compatibility, including UAC and digital signature by Microsoft.
- ^[NEW] Agent version automatic updating.

GUI features:

- File viewers for popular file formats.
- Special Email data viewer for viewing email messages in different formats including viewing attachments.
- Special Chat RTF viewer for viewing chat history in a convenient format.
- Advanced Registry and System Analyzer.
- Agent installation through Captain interface.

File System investigation features:

- View file system structure and file contents in real time.
- Quick access to shared folders, My Documents folders, installed email databases.
- Forensic file system investigation including viewing file slack, alternate data streams, etc.
- ^[NEW] Live email files, chat logs, and Internet history files in a parsed form.
- Deleted data recovery.

Data Acquisition and Export features:

- File / folder acquisition from the investigated computer.
- Logical and physical disk image creation.
- Live memory capture.
- ^[NEW] Export of parsed data from parsed email databases, chat databases, etc.

Real-time investigation features:

- Screenshots capturing.
- Running processes examination.
- The list of drivers being used.
- Running services and network sessions investigation.
- Snapshots creation.



Advanced Search features:

- Multi-parameter and multi-machine search in both file system and registry.
- ^[NEW] Advanced search in parsed email databases, chat databases, browser history, etc. Including search in email attachments, deleted data, disk unallocated space, etc.

Other features:

- Remote disk mounting.
- Set of permissions for limiting user activity inside Captain.
- Audit report with the detailed list of all operations.
- ^[NEW] Telnet for Agent remote management.

