

Ji2 ニュースレター (フォレンジック技術とEディスカバリ)

2011年8月号

はじめに

2011年6月30日に、EnCase Forensic v7がリリースされました。

EnCase Forensic v7では、新しいユーザーインターフェイスの採用、スマートフォンのデータ収集機能の追加、CPUおよびメモリ使用の最適化、HFSX, ext4ファイルシステムへの対応など、様々な変更が加えられています。今後、Ji2ではこれらの新機能に関する有効性の検証を行っていきます。

EnCaseの新しいユーザーインターフェイスは、従来とバージョンと比較して分かり易く改善されており、新たにフォレンジックを学ぶ方がEnCaseを利用される機会が増えると思われまます。今回のニュースレターでは、EnCaseを初めてご利用される方向けの情報を中心にお届け致します。

目次

1. EnCase 情報

ユーザー登録はお済みですか?.....	2
サポートポータルを活用.....	6
EnScript Analyzer	6

2. イベント情報

スマートフォン・フォレンジックトレーニング	7
NEW EnCase Advanced Forensic トレーニング	8
NEW EnCase Computer Forensic トレーニング	9

株式会社Ji2は、eDiscoveryとフォレンジックのベスト・プラクティスと社内ソリューションをご提供しています。日米企業への豊富な経験をもとに、英語と日本語でディスカバリ作業や社内インフラ構築のコンサルティングが可能です。

<http://www.ji2.co.jp>

Ji2ニュースレターは、「フォレンジック」「電子証拠開示 (eDiscovery) ディスカバリ」関連の日米最新情報を2ヶ月に1度お届けしています。

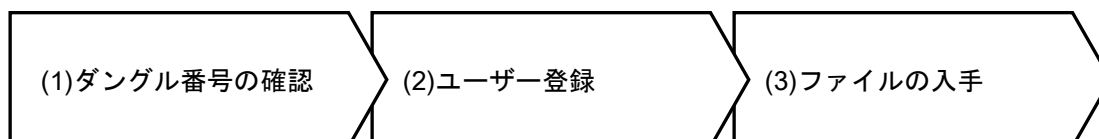
1. EnCase 情報

ユーザー登録はお済みですか？

EnCase のユーザー登録を行っておくと、製品やアップグレードに関する最新情報や、最新版のプログラムファイルをタイムリーに入手することができます。

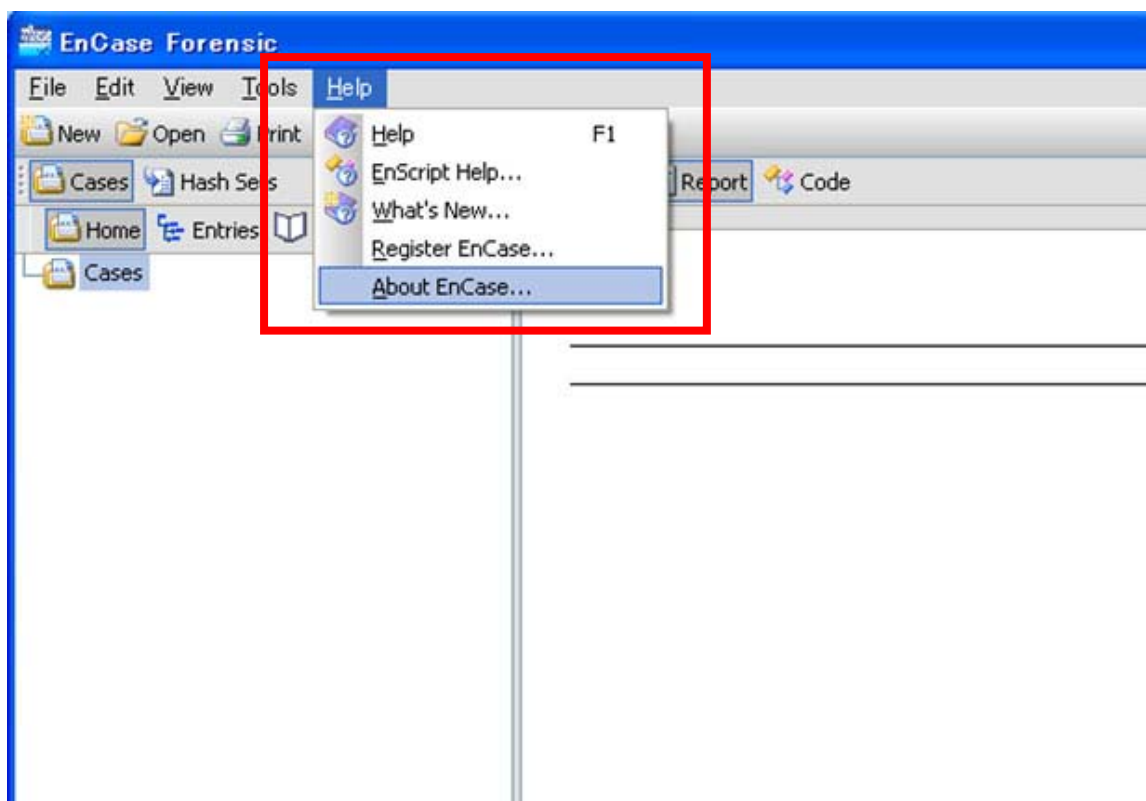
【ユーザー登録から最新のプログラム・マニュアルの入手の流れ】

ユーザー登録から最新のプログラム・マニュアル入手の流れは、(1) ダングル番号の確認、(2) ユーザー登録、(3) ファイルの入手となります。

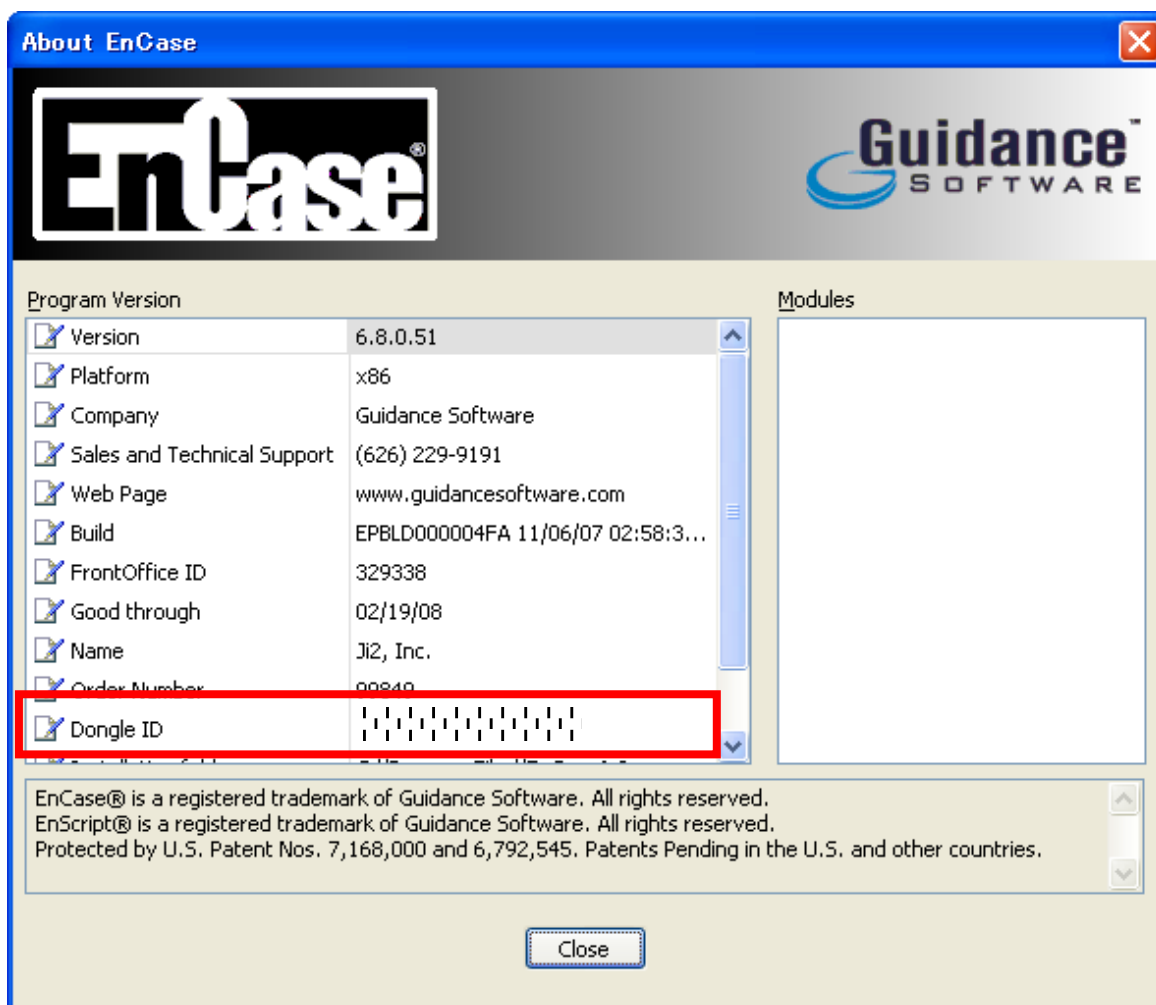


(1) ダングル番号を確認する

EnCase の画面から Help の About EnCase…をクリックすると現在の EnCase のダングル番号を確認する事が出来ます。



以下のようにダングル番号が表示されます。



(2) ウェブサイトから登録手続きを行う

下記の登録ページにアクセスし、必要な情報を入力して登録を申請します。

登録ページURL : <https://www.guidancesoftware.com/myaccount/registration.aspx>

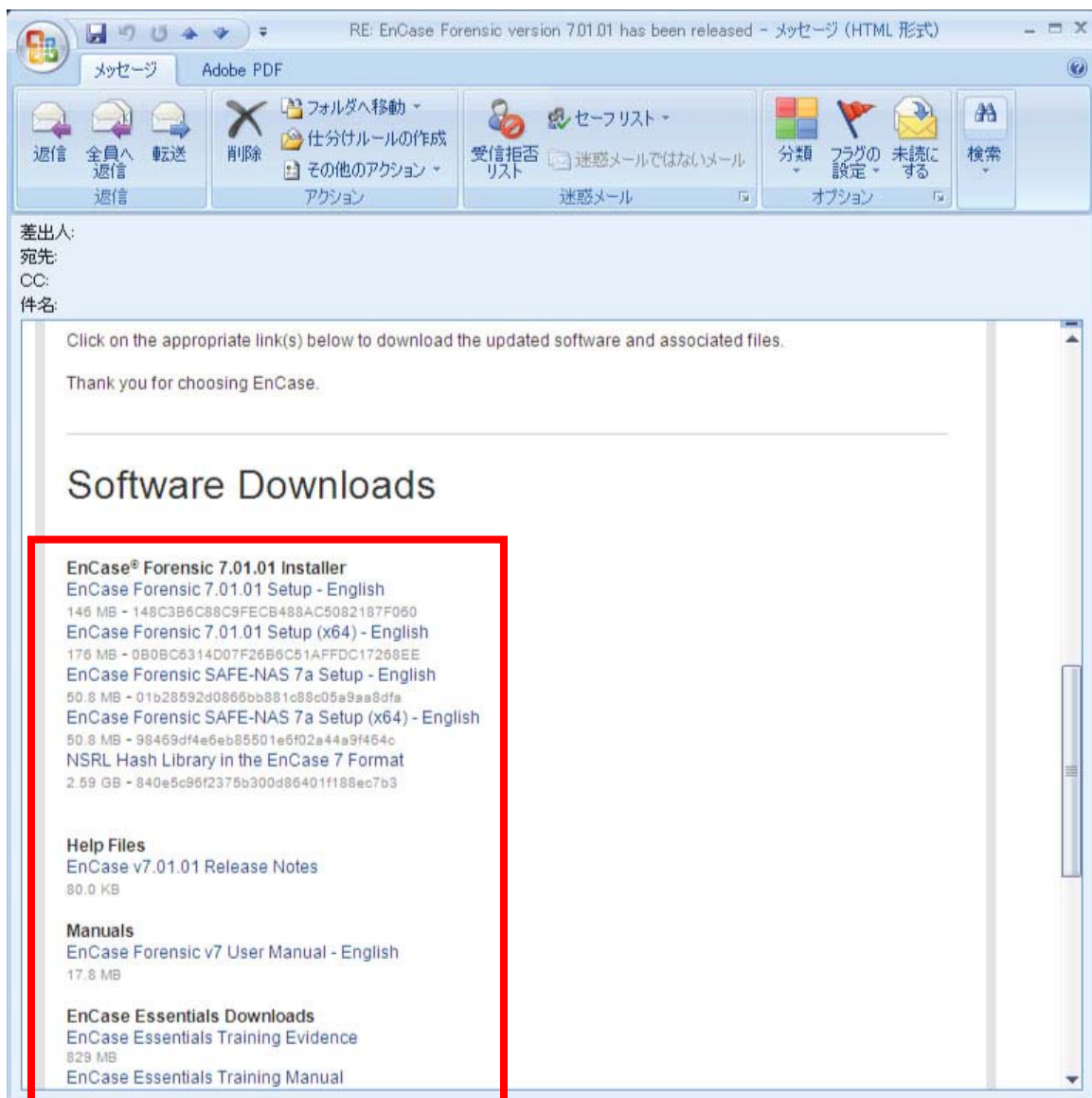
The screenshot shows the 'EnCase® Product Registration' page in a Firefox browser. The page title is 'Title Not Specified!'. The main heading is 'EnCase® Product Registration'. Below the heading, there is a note: 'Please use this form to register your EnCase software and to receive...'. A red box highlights the 'Product Serial #' and 'Email' input fields, with a callout box containing the text 'ダングル番号と登録用メールアドレスを入力'. Below this, there are radio button options for language selection. The 'Japanese' option is selected and highlighted with a red box, with a callout box containing the text '日本語を選択'. At the bottom, there is a 'SEND REGISTRATION' button highlighted with a red box, with a callout box containing the text '内容を入力してクリック'. The footer contains navigation links for Products, Services, Training, Resources, and Partners, along with social media icons and copyright information for Guidance Software, Inc. © 2011.

(3) 登録の確認と最新プログラム、マニュアルの入手

登録が完了すると、入力したメールアドレスに完了メールが送信されます。

メールには最新プログラムやマニュアルなどのダウンロードリンクが記載されています。登録が完了すると、EnCase のマイナーバージョンアップ時に、最新のセットアップファイルのダウンロードリンクが記載されたメールが届きます。

最新の最新プログラムや Cert ファイルを再度入手したいときには、上記のユーザー登録手続きをもう一度行うことで、登録ユーザーが入手可能な全てのファイルのダウンロードリンクが記載されたメールを受け取ることができます。



サポートポータルを活用

Guidance Software が運営するサポートポータルでも、EnCase に関する最新情報やプログラム、マニュアルなどの資料を入手することができます。

サポートポータルURL : <https://support.guidancesoftware.com/>

The screenshot shows a Firefox browser window displaying the Guidance Software Support Portal. The address bar shows the URL <https://support.guidancesoftware.com/>. The page header features the text "(support portal)" and the Guidance Software logo. A central "Bulletin Message" box contains the following text:

vBulletin Message

You are not logged in or you do not have permission to access this page. This could be due to one of several reasons:

1. You are not logged in. Fill in the form at the bottom of this page and try again.
2. You may not have sufficient privileges to access this page. Are you trying to edit someone else's post, access administrative features or some other privileged system?
3. If you are trying to post, the administrator may have disabled your account or, it may be awaiting activation.
4. If you need assistance from a Guidance Software technical support representative, please [contact us](#).

Below the list is a "Log in" section with the following form:

User Name:

Password:

Remember Me? [Forgotten Your Password?](#)

Log in | Reset Fields

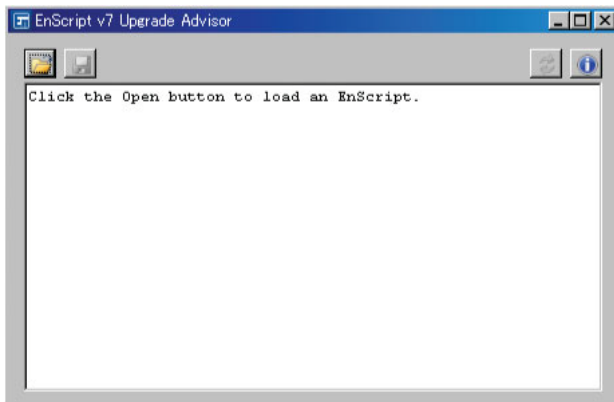
To the right of the form, it says: "If you'd like to see a preview of the portal, feel free to [take a tour](#)."

At the bottom of the message box, it states: "The administrator may have required you to [register](#) before you can view this page."

Below the message box, the text reads: "All times are GMT -7. The time now is 10:01 PM."

The footer of the page includes a "Contact Us - Top" link and the following text: "Powered by vBulletin® Version 3.8.5 Copyright ©2000 - 2011, Jelsoft Enterprises Ltd."

EnScript v7 Upgrade Advisor (中級者以上向け)



EnCase Forensic v7 のリリースに伴い、v6 用の EnScript を v7 に対応させる作業を支援するツール” EnScript v7 Upgrade Advisor” が公開されています。

EnScript v7 Upgrade Advisor はサポートポータルから入手することができます。



2. イベント情報

NEW スマートフォン・フォレンジックトレーニング

iPhone, Android等のスマートフォン・フォレンジックの最新技術、実践的な解析手法を学べるトレーニングを開講致します。

※本トレーニングは、官公庁、法執行機関様限定のトレーニングです。詳しい内容をお知りになりたい方は、弊社営業担当までお問い合わせください。

• iPhone Forensic

日時： 2011年11月8～9日（2日間）
2011年11月15～16日（2日間）
場所： 株式会社Ji2 セミナールーム

• Android Forensic

日時： 2011年11月10～11日（2日間）
2011年11月17～18日（2日間）
場所： 株式会社Ji2セミナールーム

● スマートフォン・フォレンジック お問い合わせ先

株式会社 Ji2 営業本部 佐藤能規（さとうたかのり） 電話 03-6228-0163

info@ji2.co.jp

NEW EnCase Advanced Computer Forensics

Ji2では、2011年10月にフォレンジックのエキスパートを目指す方向けの上級トレーニング「EnCase Advanced Computer Forensics」を開講致します。

このトレーニングは、ファイルシステムやOSの動作に焦点を当て、実践的な内容の実習を中心に行います。

さまざまなファイルシステムやOSの動作の理解を深めることで、Windows PC だけでなく、MAC、Linux / Unixなどの形式のコンピューターに対する高度なフォレンジック調査のアプローチが可能となります。

また講習の最終日には、EnScriptの基礎についても学び、「現状の調査業務を自動化により効率化しスピードアップを図りたい」というニーズにもお応えできる内容となっています。

【必要科目】 EnCase® Computer Forensic IIを受講し修了証を取得していること、
または EnCE® 資格保有者

【講師】 Guidance Software 社の EnCE® (外国人講師) ※逐次通訳

【日程】 2011/10/3～10/7(5日間) 9:00～18:00

【備考】 英語テキストでの受講となります

【価格】 600,000円 (税別)

【演習内容】

1. WindowsOSのNTFSアーティファクトに関する解析
2. NTFSファイルシステムにおける高度なデータリカバリー
3. Windowsイベントログファイルのリカバリーと分析
4. RAID構成をもつシステムの保全と調査
5. 暗号化の原理とリカバリー
6. Windows BitLockerボリュームの調査
7. LinuxとUnixOSのファイルシステムとアーティファクト
8. Linuxのパーティションリカバリー
9. Linuxを使ったデータ保全
10. マッキントッシュファイルシステムの構造と調査
11. マッキントッシュコンピューターのフォレンジック調査
12. MacOSXのアーティファクト
13. EnCaseによるフォレンジックメソッド応用編
14. EnScriptのプログラム

EnCase Computer Forensic トレーニング

EnCase Computer Forensic トレーニングは、EnCaseを使ったフォレンジック調査を基礎から学べるトレーニングです。初心者向けの「CF I」と中級者向け「CF II」の二部構成となっています。

- 【必要科目】** CF I : なし
CF II : CF I を修了していること
- 【講師】** CF I : Ji2所属のEnCE® (日本人講師)
CF II : Ji2所属のEnCE® (日本人講師)
- 【日程】** CF I : 2011/2/28～3/2 (4日間) 9:00～18:00
CF II : 2011/3/5～3/8 (4日間) 9:00～18:00
- 【価格】** CF I : 一般 : 400,000円 (税別) 法執行機関 : 365,000円 (税別)
CF II : 一般 : 400,000円 (税別) 法執行機関 : 365,000円 (税別)
- 【演習内容】** CF I :
1. デジタル証拠の構成とコンピュータの動きについて
 2. EnCase® によるフォレンジック調査の概要
 3. FATとNTFSファイルシステムの基本的な構造
 4. ケースの作成と、メディアのプレビューおよび取得方法
 5. 基本的なキーワード検索
 6. ファイルシグネチャ分析とファイルの確認方法
 7. 証拠データのリストア方法
 8. 分析過程で作られるデータとファイルを纏める方法
 9. 裁判所提出用証拠データの準備方法
 10. 証拠ファイルのベリファイ方法
- CF II :
1. ロジカルエビデンスファイル (LEF) の作成と利用
 2. 削除されたパーティションとファイルの発見と復元
 3. GREPを使った検索の方法
 4. EnCase® VFSとPDEの理解
 5. Windowsレジストリの理解
 6. コンパウンドファイルへの対処
 7. ファイル、ディレクトリ、ボリュームの抽出方法
 8. ハッシュとハッシュライブラリを使ったファイル特定の方法
 9. WinXPのリンクファイル、ゴミ箱、ユーザーフォルダなどの特定方法
 10. スワップファイル、スラックファイル、プリンタ印刷データの復元
 11. 印刷やFAXされたデータの回復

-
- ニュースレターの登録、解除等については、下記連絡先までご連絡ください。
 - 本ニュースレターに関するご要望、ご意見をお待ちしております。

▲ 編集・発行 ▼

株式会社 Ji2 (発行担当: 佐藤能規)

E-mail: newsletter@ji2.co.jp

米国事務所: 11235 Knott Ave. Suite C. Cypress, CA 90630 U.S.A.

日本事務所: 〒160-0022 東京都新宿区新宿 1-9-5 大台ビル 3F

TEL: 03-6228-0163 FAX: 03-6228-0164 <http://www.ji2.co.jp/>
