

PI Option Overview

The tool set is based around 10 years of active development and distribution - first to intelligence agencies, then military Intel agencies, and later to law enforcement, internationally.

The following list shows the general descriptions of the tool's capabilities at a top level of comparison. Several hundred unique and fast operations are contained within the codebase. The application itself is written in 4 different programming languages, fitted together under a 100% managed Dotnet Studio 2005/2008 codebase. Many of the components used in the making of the tool have no commercial counterparts either in commercial forensics tools or closed shop Intel tools.

There are 5 tool-specific development areas, not existing in any computer forensics or investigative tool:

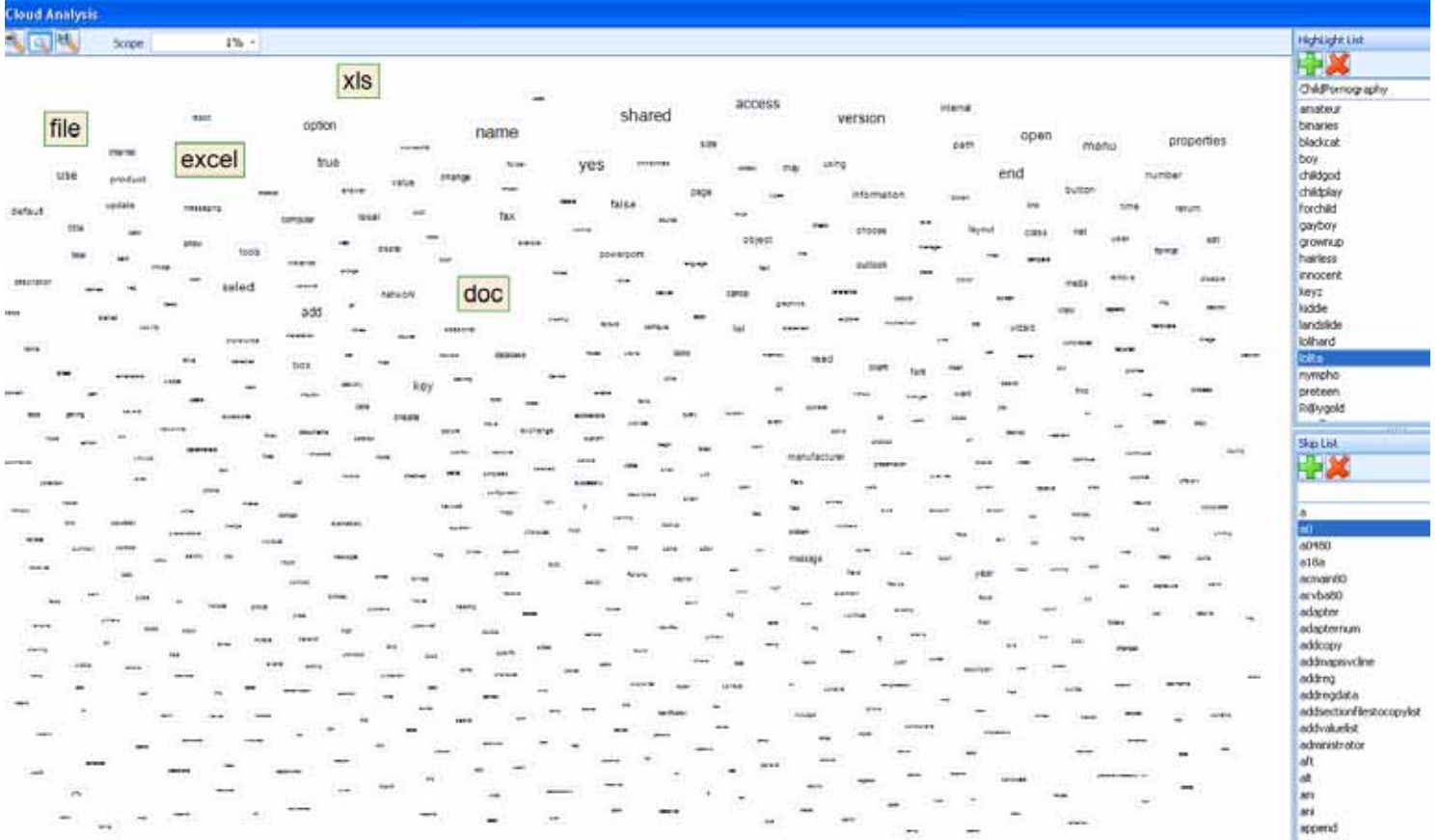
The first is the ability for the user to integrate 100% compliant programming languages into the application base.

Below you can see screenshots of the code generation editor. It is 100% Dotnet C# and VB.net compliant and allows, for the first time in any toolset, the ability for the user to have 100% management of the resources programmatically, and also, for the first time, to use the application base as an extensible programming environment all on its own. Using this tool alone, there is no longer a need in forensics to own another programming environment for any tasks, much less common ones. It is also designed to allow integration of the key build components within the tool chain so that purchases of outside Net Controls or DB engines (like the built-in Microsoft SQL Server 2008 64 bit engine) can be avoided as long as the user stays within the application base. The user would have little or no reason to ever step outside that base in normal forensics challenges.

```
1 Imports System
2 Imports System.IO
3 Imports System.Drawing
4 Imports MiniAppLiaison
5 Imports System.Text
6 Imports Microsoft.VisualBasic.Interaction
7 Imports Microsoft.VisualBasic
8
9 ' This test app is a demo
10
11 Namespace MiniApp
12 Friend Class App
13 Private WithEvents imald As MiniAppLiaison, ILookMiniAppLiaison
14
15 ' WARNING: As this function bypasses all of the checks in the media wizard it is up to you to validate that the media
16 ' and that the image types are formats that can be processed.
17
18 Namespace MiniApp
19 Friend Class App
20 Private WithEvents imald As MiniAppLiaison, IMiniAppLiaison
21
22 Public Function Main(ByRef Iimald As MiniAppLiaison, IMiniAppLiaison) As Integer
23     imald = Iimald
24     Dim ImageSetList() As Arraylist
25     Dim FileName, Textline As String
26     Dim ofd As New OpenFileDialog
27     ' Get the bulk image set list file
28     ofd.Title = "Select the BIL file"
29     ofd.Filter = "All files (*.*)|*.|Bulk Image Set list (*.bil)|*.bil"
30     ofd.FilterIndex = 2
31     ofd.InitialDirectory = "c:\\"
32     ofd.DefaultExt = ".bil"
33     ofd.FileName = ""
34     If ofd.ShowDialog() = DialogResult.Cancel Then Exit Function
35     FileName = ofd.FileName
36     If FileName = "" Then Exit Function
37     System.Windows.Forms.Application.DoEvents()
38     Dim FH As Integer = FreeFile()
39     FileOpen(FH, FileName, OpenMode.Input, OpenAccess.Read)
40     While Not EOF(FH) ' Loop until end of file
41         Textline = LineInput(FH).Trim ' Read line into variable.
42         If Textline <> "" Then
43             If Textline.StartsWith("-") Then
44                 ' Image set continuation
```

For the first time in any forensics toolset, there is also the integration of an analytics package of functions and globalization artificial intelligence derivatives, which bring computer forensics to the forefront of its investigative abilities.

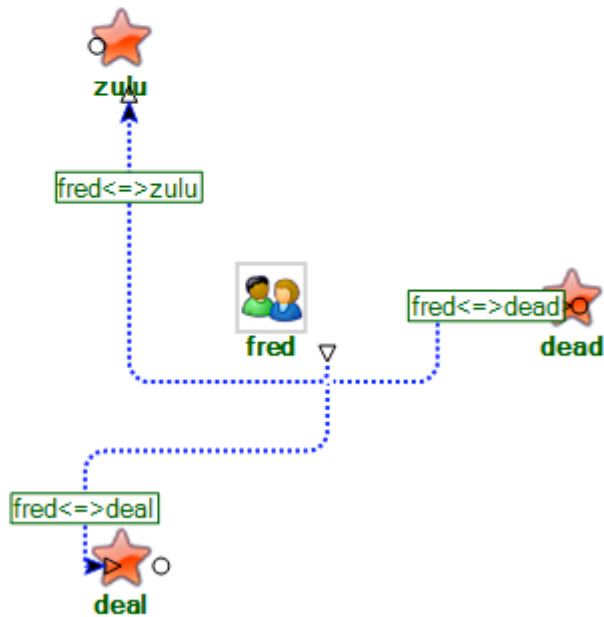
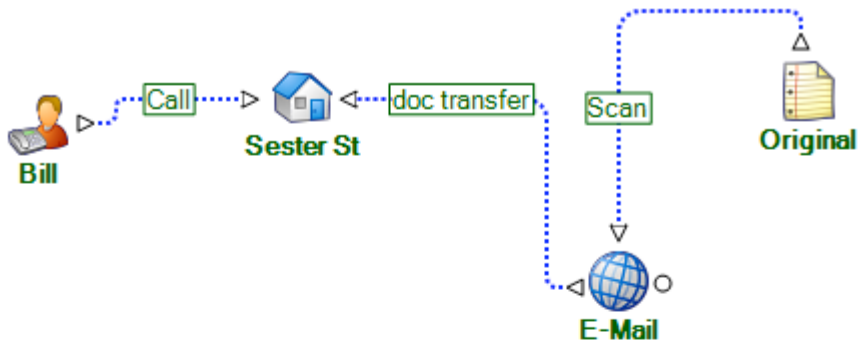
Below is a "Cloud" analytics view, which makes simple work of word relationships from tens of millions of indexed words in single or multiple-analyzed computer systems. Here, you see the word relationships elevating themselves through mathematics into human recognizable and visible keys as to their frequencies and relationships within the digital data band examined.



The third area, only existing in this tool set, is the Lead Analysis integration. No other tools have these designed and integrated analytics tools at any level, much less at such a clear functioning level to show evidence relationships among all of the data subjects of the entire digital data being processed.

This type of analytic ability is only contained in analytics data tools that cost several thousand dollars alone. However, even in the standalone toolsets, there is no data integration built into the digital forensics equation. Those tools require the data to be exported first, which is a very time consuming job requiring immense amounts of storage, data extraction elapsed time - as well as import time, before they can achieve solutions anywhere close to the integration shown in the next 3 screens.

The screenshot displays the 'Lead Analysis' software interface. On the left, a vertical sidebar lists 'Lead Objects' including Comms, Computer, E-Mail, Info, People, Places, and Web. The central 'Canvas' area shows a network diagram with nodes: 'Bill' (person icon), 'Sester St' (house icon), 'E-Mail' (globe icon), and 'Original' (document icon). Dotted arrows connect 'Bill' to 'Call', 'Call' to 'Sester St', 'Sester St' to 'doc transfer', 'doc transfer' to 'Scan', and 'Scan' to 'E-Mail'. A dashed arrow also connects 'Original' to 'E-Mail'. Below the diagram is a 'fred' icon. On the right, the 'Potential Links' panel is empty. Below it, the 'Skip List' panel shows a search filter 'A' and a list of results including 'a', 'a_e', 'a0', 'a0480', 'a1', 'a18a', 'a2', 'a21', 'a29', 'a3', 'a4', 'a5', 'aa123', 'aact' (highlighted), 'acmain80', 'acvba80', 'adapter', 'adapternum', 'adapternumber', 'adapteroptions', 'adapters', 'addcopy', and 'addmapisvcline'.



The following screen shows a capability that has never existed in digital forensics at any level, in any tool, or in any organization. Without explanation, it is easy to miss the utter complexity, unparalleled uniqueness, and intrinsic value in the capability.

Computer forensics at any level, criminal, civil, regulatory or intelligence operations all have to handle one thing they simply have no tools to deal with. They all have the same exact demand for this capability, yet none would invest in the technology to solve the issue. The issue is external nefarious command and control over computer processes on any machine, anywhere, at any time and without recourse by almost any user. The missing link in the forensics chain is also it's weakest link : Virus contaminants!

Most people – except members of the defense bar – would be pressed to believe that issue. After all, most people presume the government prosecutors would willingly protect a defendant’s rights. They would presume any doubt as to culpability would be a digital fact that the government or civil litigants would not fail to raise as defenses in either civil or criminal cases.

Yet such capability does not exist in any tool but this one. A forensics tool works not with computers, but data images of computers already made by other processes. Through the investigator, the tools examine the systems at a different level than that of a normal user, in order to determine the inculpatory, or important data or evidence contained within that system substitute. This is the point of the “broken link” hinge pin of digital forensics.


So why is something of such importance missing from tools at the commercial level? The issue is that none of the other two tools have a method to integrate the scanning of files within an image container, without first removing the files from the image itself and placing them on a disk, hence the conundrum. If they remove it by copying it from inside an image into the host filesystem, they immediately fall victim to any AV software externally running on the host forensics machine. This is not the only issue. The other issue is that very complete AV software is expensive, and was not designed with computer forensics in mind. It was designed for interception and identification of Viruses, Trojans and other malware to be “found” in a mode and form which the AV software could understand. This is not the case with computer images of other systems. Therefore, the processing by outside or external tools is immensely time consuming and expensive.

In the current tool below, you will see the simple interface presentation of the identification of virus contaminants within an image container. The red bug icon represents the presence of a virus or malware in that particular object file.

Why is the issue so important otherwise? In order to examine data from computer systems, invariably, the examiner needs different sets of reviewers to further decide the implications of what is found. This could be legal professionals, the courts, or even a witness. In others, to get the data into a container and then move the container in an encrypted form out to reviewers, it was necessary that viruses COULD NOT – MUST NOT contaminate the recipients system, just during the review process. This is accomplished, in the only method existing for any digital tool, by the elimination of the contaminants at first light, while still in the image, before they can be transferred to any other system. The release in the wild of just one email virus, during the examination of a criminal case that is centered on the virus to begin with, would collapse the entire case and could result in civil liabilities of unknown proportions.

The conviction of an innocent person has no intrinsic value of dollars in the legal system of any country. It far exceeds the value of money and goes to the heart of what is both good and bad about investigative processes that fail to adequately protect the rights of the accused.

Name	Size	Tag	Type	Created	Last Accessed	Last Modified	Attributes
bskrv11a_base_e9e91478c16f31d585d5724bbf7797b...	105,852		7z	01/Feb/2008 11:32:59	01/Feb/2008 11:32:59	17/Jul/2007 00:54:57	
bskrv11a_pwd=doyle_make_sfx_type_winrar_ff626...	219,752		exe	01/Feb/2008 11:32:59	01/Feb/2008 11:32:59	17/Jul/2007 04:30:05	
bskrv11a_pwd=doyle_type_winrar_9e31e3c672d9e6...	116,840		rar	01/Feb/2008 11:32:59	01/Feb/2008 11:32:59	17/Jul/2007 04:28:50	
contents this device.htm	78,929		htm	26/Aug/2007 02:11:06	26/Aug/2007 00:00:00	26/Aug/2007 02:10:18	A---
-D\$105.TMP	33,900		tmp	26/Aug/2007 00:45:26	26/Aug/2007 00:00:00	26/Aug/2007 00:45:30	A---
-D\$107.TMP	54,481		tmp	26/Aug/2007 00:46:22	26/Aug/2007 00:00:00	26/Aug/2007 00:46:24	A---
decon	0			25/Aug/2007 23:52:04	25/Aug/2007 00:00:00	25/Aug/2007 23:52:06	A---
decon ntuser.dat.7z ilook v8	499,485		7z	16/Aug/2007 18:49:46	25/Aug/2007 00:00:00	16/Aug/2007 18:49:50	A---
7z	1,232,783		7z	14/Aug/2007 20:38:32	26/Aug/2007 00:00:00	14/Aug/2007 20:40:04	A---
-EGIST~1.PDF	0		pdf	25/Aug/2007 23:51:40	25/Aug/2007 00:00:00	25/Aug/2007 23:51:42	A---
eicar _ THE ANTI-VIRUS OR ANTI-MALWARE TEST FIL...	23,177		pdf	25/Aug/2007 02:50:00	25/Aug/2007 00:00:00	25/Aug/2007 02:50:00	A---
eicar.com	68		com	01/Feb/2008 11:33:08	01/Feb/2008 11:33:08	24/May/2000 19:07:00	
EICAR.COM	68		com	26/Aug/2007 02:07:34	26/Aug/2007 00:00:00	25/Aug/2007 02:23:08	A---
eicar.com.txt	68		txt	26/Aug/2007 02:07:34	26/Aug/2007 00:00:00	25/Aug/2007 02:23:24	A---
eicar_com.zip	184		zip	26/Aug/2007 02:07:34	26/Aug/2007 00:00:00	25/Aug/2007 02:23:26	A---
eicar_com.zip	184		zip	01/Feb/2008 11:33:07	01/Feb/2008 11:33:07	11/Jul/2000 21:33:36	
eicarcom2.zip	308		zip	26/Aug/2007 02:07:34	26/Aug/2007 00:00:00	25/Aug/2007 02:23:34	A---
EICARgen «	54,481		pdf	26/Aug/2007 00:46:22	26/Aug/2007 00:00:00	26/Aug/2007 00:46:24	A---
EICARgen.c	1,402		c	01/Feb/2008 11:33:05	01/Feb/2008 11:33:05	21/Nov/2006 21:22:30	

Property	Value
File	eicar.com.txt
Top Level Parent	ewqr (0)
Key	4469344 / 4469320.0.15.19
Barcode	
Type	txt
Extra Info	
DOS	EICARC~1.TXT
Path	\virus
Created	26 August 2007 02:07:34
Last Accessed	26 August 2007 00:00:00
Last Modified	25 August 2007 02:23:24
Virus/Trojan found	Eicar-Test-Signature
Truncated	No
Attributes	A---
Stream (0)	Default
Stream Size	68
Allocation	4,096
Run.0000; type 0	13,052 for 8
Undeleted	No
Indexed	No
Tagged	No

Viewer Hex View **Properties** Log Search History

The fifth item unique to this tool is the distinguishing ability to time like computer system events into real understandable human terms. The processes that are exposed by the detail options below are unique to this tool and easily understood by lay people, and the presentation itself encompasses the ability to integrate any set of fact data in a timeline form across the image data source system being investigated.

