RELAZIONE TECNICA DI PARTE SUL SUPPORTO MAGNETICO DEL COMPUTER APPLE MAC BOOK PRO IN USO A RAFFAELE SOLLECITO E SEQUESTRATO DALLA AUORITA' GIUDIZIARIA IN DATA 06 NOVEMBRE 007.

PREMESSA

I sottoscritti dott. Michele GIGLI e Antonio D'AMBROSIO tecnici incaricati dalla difesa di Raffaele SOLLECITO imputato nel procedimento penale n°9066/07 hanno effettuato un'analisi sul supporto magnetico del computer in uso a Raffaele Sollecito. All'uopo hanno utilizzato n.2 copie immagine: la prima ottenuta con un software encase dalla Polizia Postale di Perugia e la seconda ottenuta dalla società Kroll Ontrack presso gli uffici del Tribunale di Perugia, previa autorizzazione del sig. Presidente di Corte d'Assise, con strumentazione certificata. Il lavoro è stato effettuato analizzando i file di sistema presenti su un copia del supporto magnetico del dott. Raffaele Sollecito e incrociando i risultati con l'export generato dal software forense EnCasec 6.8. L'intento era di rispondere ai seguenti quesiti:

Verifichi il consulente se per i seguenti periodi di tempo vi sia stata interazione umana sul computer Apple MacBooK Pro, sequestrato a Raffaele SOLLECITO in data 6 novembre 2007, analizzando l'Hard Disk acquisito in copia forense, nonchè i files di log acquisiti dalla Polizia Postale dalla società Fastweb e in caso positivo indichi la tipologia dell'attività posta in essere:

-1 DALLE ORE 15 ALLE ORE 18.30 DEL GIORNO 30 OTTOBRE 2007
-2 DALLE ORE 22.00 ALLE ORE 5.00 DEI GIORNI 01-02 NOVEMBRE 2007
-3 DALLE ORE 11.30 ALLE ORE 12.30 DEL GIORNO 02 NOVEMBRE 2007
-4 DALLE ORE 22.00 ALLE ORE 13.30 DEI GIORNI 05-06 NOVEMBRE 2007

-1 DALLE ORE 15 ALLE ORE 18.30 DEL GIORNO 30 OTTOBRE 2007

Analisi dei dati relativa alle attività svolte il giorno 30 Ottobre 2007 dalle ore 15:00 alle ore 18:30

Al fine di stabilire l'interattività umana sul computer in questione, siamo partiti dalla lettura del file generato con il software forense EnCase 6.8 e incrocio di tali dati con quelli recuperati da una copia del disco dello stesso computer, relativamente al periodo compreso tra le ore 15.29 del 30 Ottobre 2007 e le 18:30 dello stesso giorno. Abbiamo rilevato una intensa interazione umana sia su applicativi del personal computer, che su applicativi che richiedono collegamento alla rete internet. Tutti gli applicativi interessati da queste attività sono i seguenti:

Nome applicazione	Tipologia
Skype	Chat – VoIP
Messenger	Chat
iTunes	Lettore Multimediale
Adobe Acrobat Professional	Editing PDF
Apple Mail	Client posta elettronica
Apple Safari	Browser WEB

Tabella 1

L'interazione umana inizia alle ore 15.29 rilevabile dal file encase FILES 25-10_3-11-2007.xls (allegato A) dalla riga 2342 alla riga 2347, che indica attività con Skype. Questo è un programma di Instant Messaging, il quale permette di comunicare con altro utente, sia a mezzo chat che con voice. L'interazione continua con le righe successive dalla 2348 alla 2385 con il programma Microsoft Messenger, che permette le stesse modalità di comunicazione di Skipe.

Continua con:

Safari

Le attività di maggior rilievo ed interesse le abbiamo individuate analizzando la cronologia di Safari contenuta nel file History.plist che è reperibile al path */Volumes/MacOS HD/Users/macbookpro/Library/Safari/History.plist*. Il file può essere aperto utilizzando l'applicazione "Textedit" o "Property List Editor" dell'Apple Developers Tool; a seguire uno stralcio dell'**Allegato B** contenente le righe del periodo in questione dove si può leggere l'URL della pagina web aperta con a seguire la data e l'ora dell'accesso. Si fa notare che Safari riporta la data in formato Timestamp *(Il timestamp o "marca temporale" è una sequenza di caratteri che rappresentano una data e/o un orario per accertare l'effettivo avvenimento di un certo evento. La data è di solito presentata in un formato consistente, in modo che sia facile da comparare con un'altra per stabilirne l'ordine temporale. La pratica dell'applicazione di tale marca temporale è detto timestamping. Il formato timestamp è utile perchè utilizzando il tipo di dati INT ti permette di manipolare facilmente le date e memorizzarle in un database. Il numero timestamp esprime quanti secondi sono passati dal 1 gennaio 1970)* e che noi abbiamo tradotto con una utility in formato internazionale di facile lettura e riportato col colore rosso.

Se leggiamo i dati partendo dall'ultimo link che in ordine temporale è il primo (03:59:27 p.m. del 30 ottobre), notiamo che sono stati visitati diversi siti con motori di ricerca (www.google.it, www.youtube.com,) nei quali sono state effettuate delle ricerche e successivamente aperte le pagine suggerite dalla ricerca.

Tutte le immagini che abbiamo allegato sono state ottenute copiando gli URL presenti nel codice al fine di riprodurre le azioni eseguite sul computer in esame. Avendo riprodotto tali operazioni a distanza di 22 mesi dal momento in cui sono state realmente eseguite, ci aspettavamo delle differenze dovute all'evoluzione continua del web; le risposte ottenute nella riproduzione delle azioni risultano invece perfettamente conformi a quanto realmente accaduto nel periodo in esame, infatti i motori di ricerca ripropongono come risultato link le stesse pagine che troviamo nella History.

Di seguito riportiamo in dettaglio le operazioni di questo periodo (vedi allegato B).

Le seguenti istruzioni indicano che sul motore di ricerca www.youtube.com è stata effettuata una ricerca utilizzando le parole chiave *"balla coi lapi";* il risultato della ricerca è visibile nella "figura 1"

<dict>
<key></key>
<string>http://www.youtube.com/results?search_query=balla+coi+lapi&search=Search</string>
<key>lastVisitedDate</key>
<string>215449167.7</string> > Tuesday 30 October 2007 03:59:27 PM <
<key>title</key>
<string>YouTube - Broadcast Yourself.</string>
<key>visitCount</key>
<integer>1</integer>
</dict>

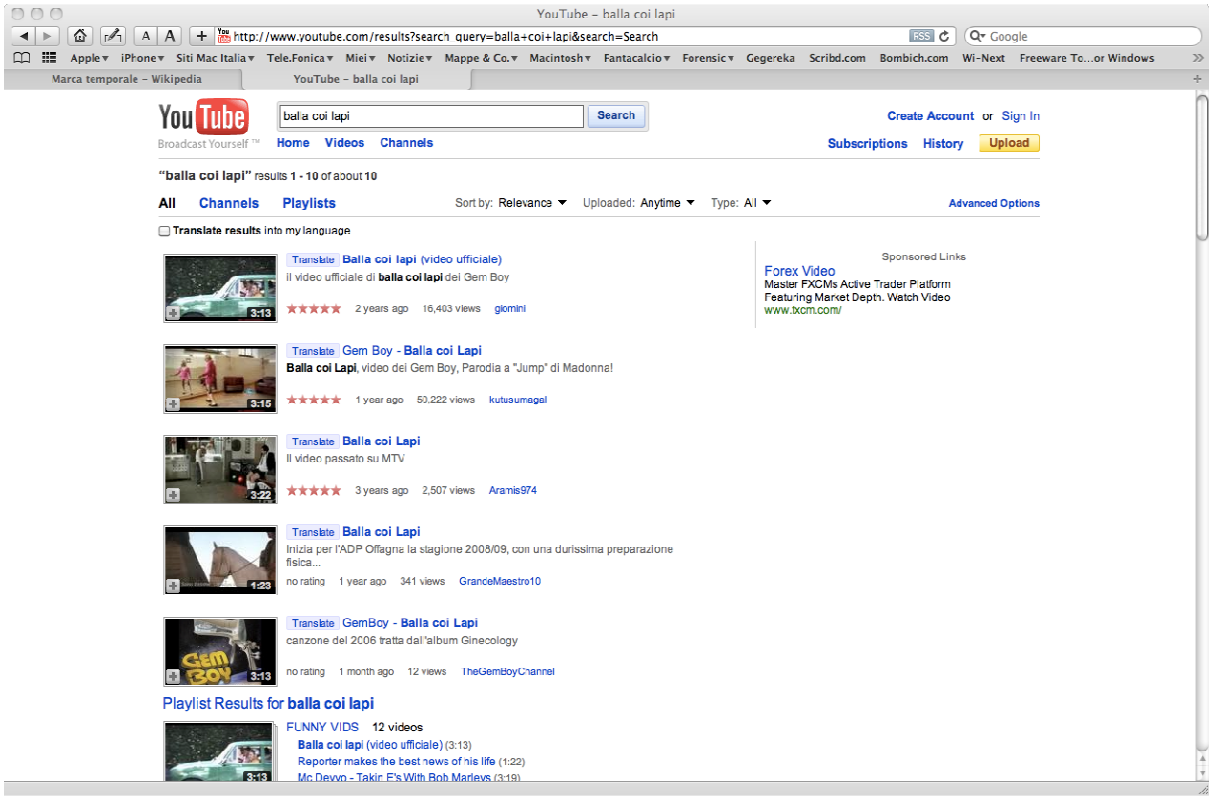

fig. 1

Poi è stato selezionato il secondo dei video dell'elenco e visualizzato il video dal nome *"Balla coi lapi (video ufficiale)"* del gruppo musicale Gem Boy code illustrato nella "figura 2".

<dict>
<key></key>
<string>http://www.youtube.com/watch?v=vdwo4bNmNh4</string>
<key>lastVisitedDate</key>
<string>215449173.0</string> > Tuesday 30 October 2007 03:59:33 PM <
<key>title</key>
<string>YouTube - Balla coi lapi (video ufficiale)</string>
<key>visitCount</key>
<integer>1</integer>
</dict>

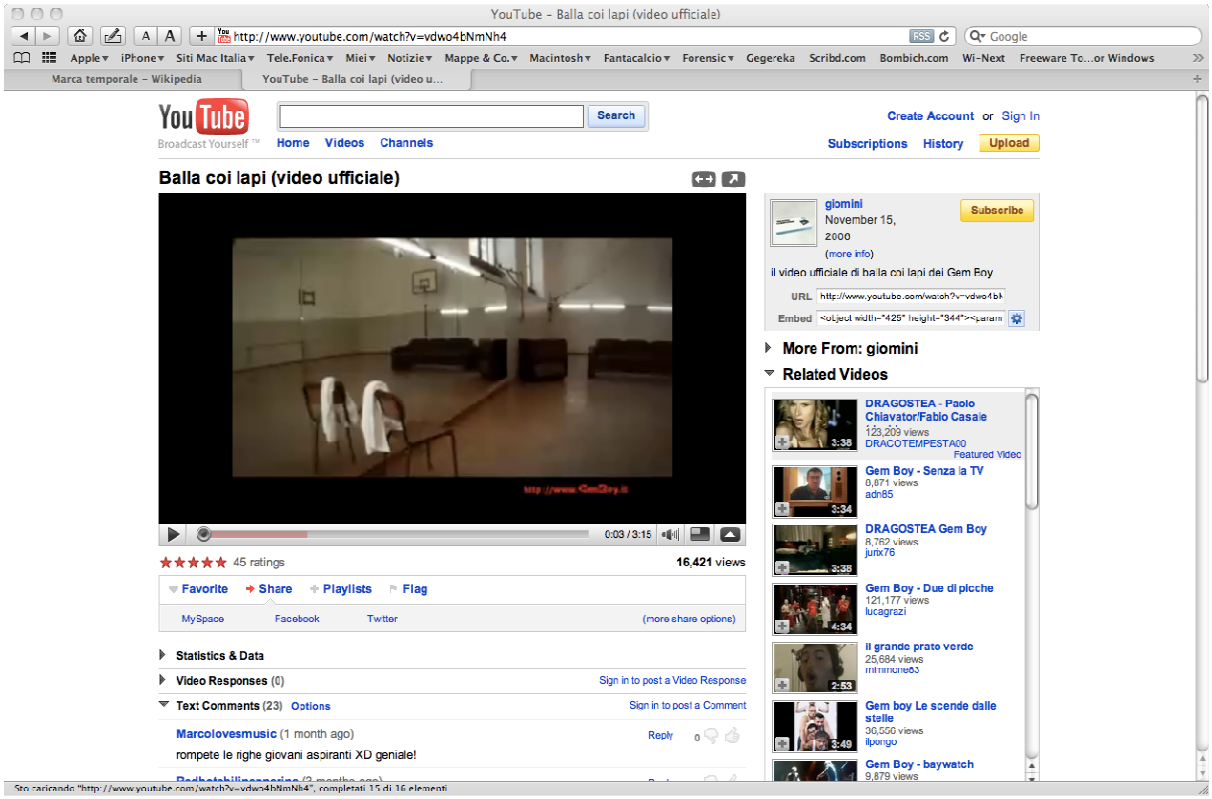

fig. 2

Terminata la visualizzazione di un video, YouTube fornisce sempre dei suggerimenti a video correlati a quello appena visionato, infatti la pagina successiva fa riferimento al video parodia della canzone "*Just my immagination*" dello stesso gruppo Gem Boy.

<dict>
<key></key>
<string>http://www.youtube.com/watch?v=5KXG1a96Vhg</string>
<key>lastVisitedDate</key>
<string>215450019.8</string> > Tuesday 30 October 2007 04:13:39 PM <
<key>title</key>
<string>YouTube - dragonball just my immagination-gem boy</string>
<key>visitCount</key>
<integer>1</integer>
</dict>

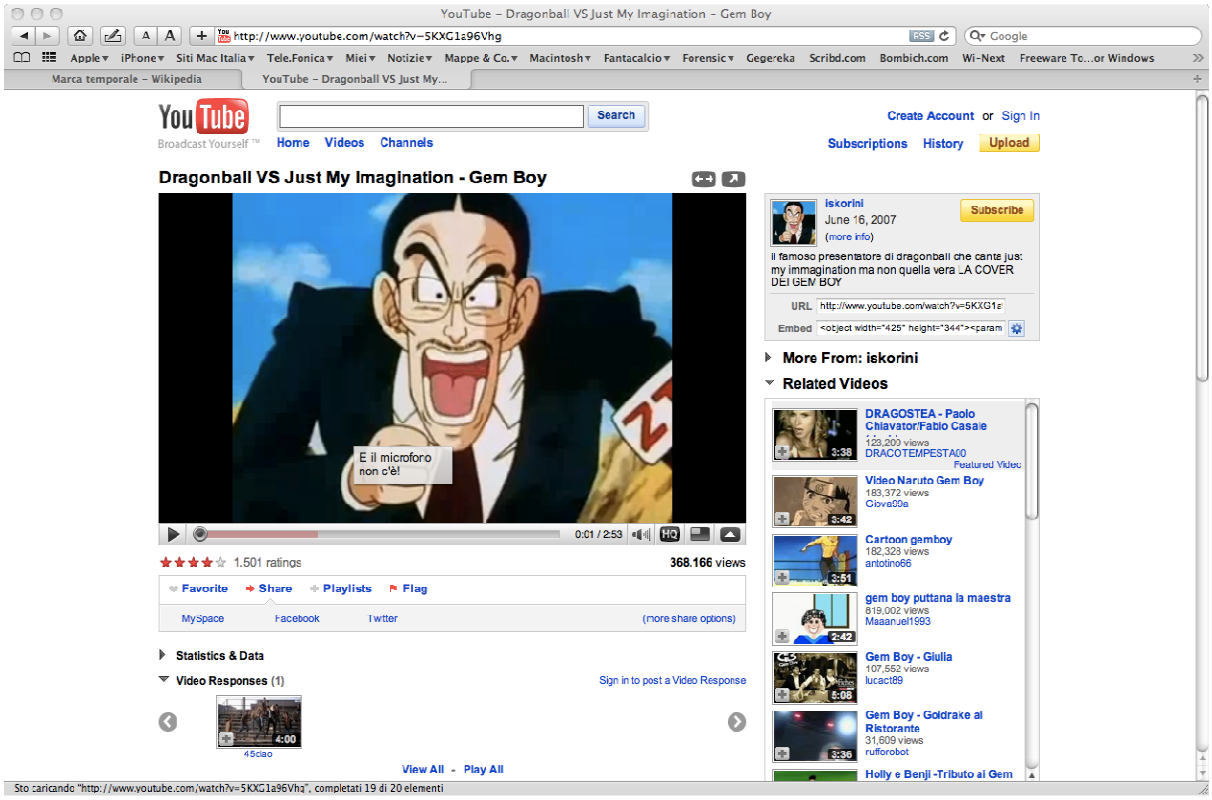

fig. 3

Infine è stato guardato un altro video dove un gruppo di ragazzi riproduce lo stesso brano, presumibilmente trovato tra i video suggeriti dallo stesso YouTube

<dict>
<key></key>
<string>http://www.youtube.com/watch?v=up4K0TrpXFo</string>
<key>lastVisitedDate</key>
<string>215450190.1</string> > Tuesday 30 October 2007 04:16:30 PM <
<key>title</key>
<string>YouTube - just my immagination - gita a Monaco</string>
<key>visitCount</key>
<integer>1</integer>
</dict>

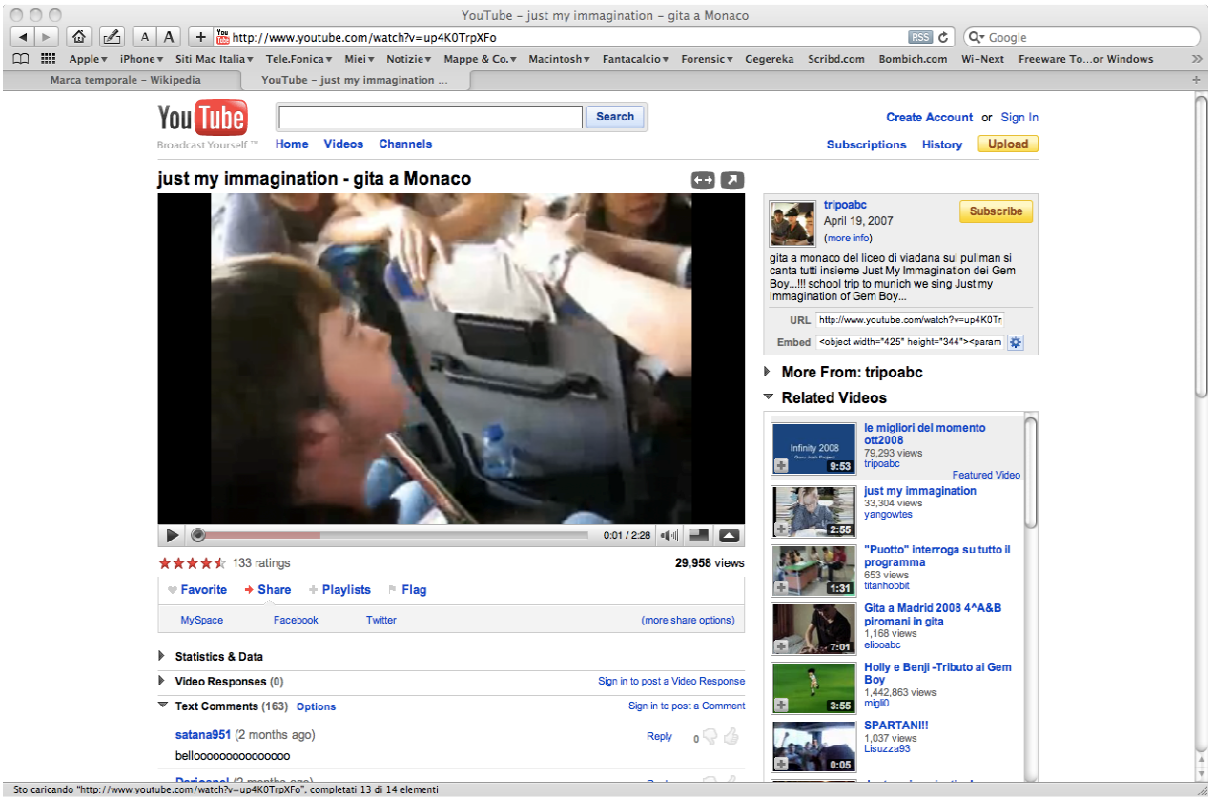

fig. 4

Le istruzioni relative alle 8 pagine successive fanno riferimento al portale di "Windows Live Hotmail", infatti la figura 5 mostra la pagina di log-in ottenuta sempre copiando uno degli URL.

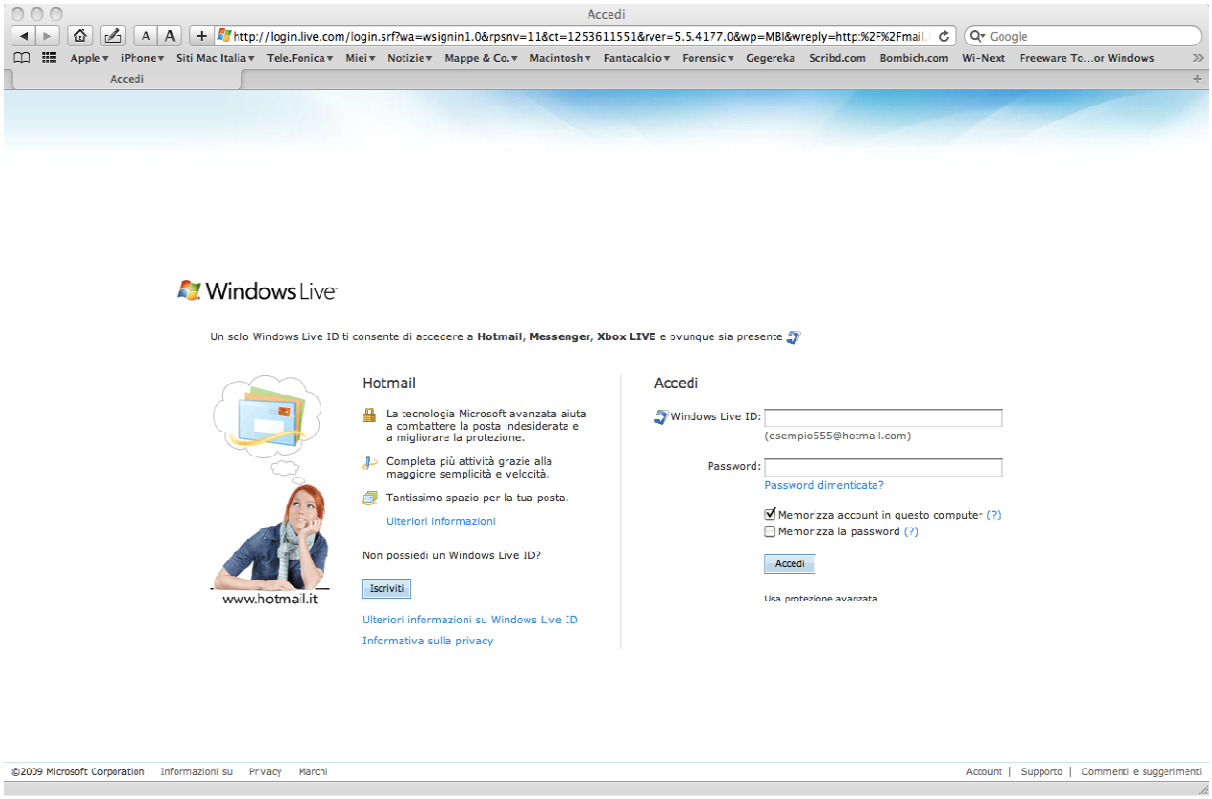

fig. 5

Effettuando il log-in con un account in nostro possesso, sono state simulate le operazioni presenti nel codice e abbiamo rilevato che sono state effettuate operazioni di lettura e cancellazione di mail.

<dict>
<key></key>
<string>http://by105w.bay105.mail.live.com/mail/ReadMessageLight.aspx?ReadMessageId=f3229091-98c5-4d39-ae42-744a6fd4195d&n=268719254</string>
<key>lastVisitedDate</key>
<string>215450799.7</string> > Tuesday 30 October 2007 04:26:39 PM <
<key>title</key>
<string>Windows Live Hotmail</string>
<key>visitCount</key>
<integer>2</integer>
</dict>

<dict>
<key></key>
<string>http://by105w.bay105.mail.live.com/mail/ReadMessageLight.aspx?AllowUnsafe=True&FolderID=00000000-0000-0000-0000-000000000001&ReadMessageId=f3229091-98c5-4d39-ae42-744a6fd4195d&n=2010118319</string>
<key>lastVisitedDate</key>
<string>215450950.7</string> > Tuesday 30 October 2007 04:29:10 PM <
<key>title</key>
<string>Windows Live Hotmail</string>
<key>visitCount</key>
<integer>1</integer>
</dict>

<dict>
<key></key>
<string>http://by105w.bay105.mail.live.com/mail/ReadMessageLight.aspx?Action=DeleteMessage&FolderID=00000000-0000-0000-0000-000000000001&ReadMessageId=f3229091-98c5-4d39-ae42-744a6fd4195d&n=2092401925</string>
<key>lastVisitedDate</key>
<string>215451057.2</string> > Tuesday 30 October 2007 04:30:57 PM <
<key>title</key>
<string>Windows Live Hotmail</string>
<key>visitCount</key>
<integer>1</integer>
</dict>

<dict>
<key></key>
<string>http://by105w.bay105.mail.live.com/mail/ReadMessageLight.aspx?Action=DeleteMessage&FolderID=00000000-0000-0000-0000-000000000001&ReadMessageId=d7f36c81-6c91-4fa3-8494-2a2a7e6845b9&n=1588424349</string>
<key>lastVisitedDate</key>
<string>215452234.8</string> > Tuesday 30 October 2007 04:50:34 PM <
<key>title</key>
<string>Windows Live Hotmail</string>
<key>visitCount</key>
<integer>1</integer>
</dict>

<dict>
<key></key>
<string>http://by105w.bay105.mail.live.com/mail/ReadMessageLight.aspx?Action=DeleteMessage&FolderID=00000000-0000-0000-0000-000000000001&ReadMessageId=4c4bd0a1-8f6c-4a6a-b220-711b688d9db0&n=397660841</string>
<key>lastVisitedDate</key>
<string>215452241.2</string> > Tuesday 30 October 2007 04:50:41 PM <
<key>title</key>
<string>Windows Live Hotmail</string>
<key>visitCount</key>
<integer>1</integer>
</dict>

<dict>
<key></key>
<string>http://by105w.bay105.mail.live.com/mail/ReadMessageLight.aspx?AllowUnsafe=True&FolderID=00000000-0000-0000-0000-000000000001&ReadMessageId=ac629c02-0d57-4727-9538-6af0c9d41a25&n=1463511969</string>
<key>lastVisitedDate</key>
<string>215452248.7</string> > Tuesday 30 October 2007 04:50:48 PM <
<key>title</key>
<string>Windows Live Hotmail</string>
<key>visitCount</key>

<integer>1</integer>
</dict>

<dict>
<key></key>
<string>http://by105w.bay105.mail.live.com/mail/ReadMessageLight.aspx?Action=DeleteMessage&FolderID=00000000-0000-0000-0000-000000000001&ReadMessageId=ac629c02-0d57-4727-9538-6af0c9d41a25&n=2012208481</string>
<key>lastVisitedDate</key>
<string>215452253.0</string> > Tuesday 30 October 2007 04:50:53 PM <
<key>title</key>
<string>Windows Live Hotmail</string>
<key>visitCount</key>
<integer>1</integer>
</dict>

</dict>
<key></key>
<string>http://by105w.bay105.mail.live.com/mail/ReadMessageLight.aspx?AllowUnsafe=True&FolderID=00000000-0000-0000-0000-000000000001&ReadMessageId=5c4f761d-1e6e-4c60-a2e5-c3571b40985a&n=396515141</string>
<key>lastVisitedDate</key>
<string>215452258.2</string> > Tuesday 30 October 2007 04:50:58 PM <
<key>title</key>
<string>Windows Live Hotmail</string>
<key>visitCount</key>
<integer>1</integer>
</dict>

Questa porzione di codice ci riporta a una ricerca effettuata su google.it delle parole chiavi *"automatically defined functions"*; il risultato della ricerca è mostrato nella figura 6; le istruzioni che seguono sono tutti link di questa ricerca come mostrato anche dal diverso colore di alcuni di loro. I browser, infatti, individuano con un colore differente i collegamenti ipertestuali dopo che questi sono stati aperti.

<dict>
<key></key>
<string>http://www.google.it/search?source=ig&hl=it&rlz=&q=automatically+defined+functions&btnG=Cerca+con+Google&meta=</string>
<key>lastVisitedDate</key>
<string>215452338.5</string> > Tuesday 30 October 2007 04:52:18 PM <
<key>title</key>
<string>automatically defined functions - Cerca con Google</string>
<key>visitCount</key>
<integer>1</integer>
</dict>

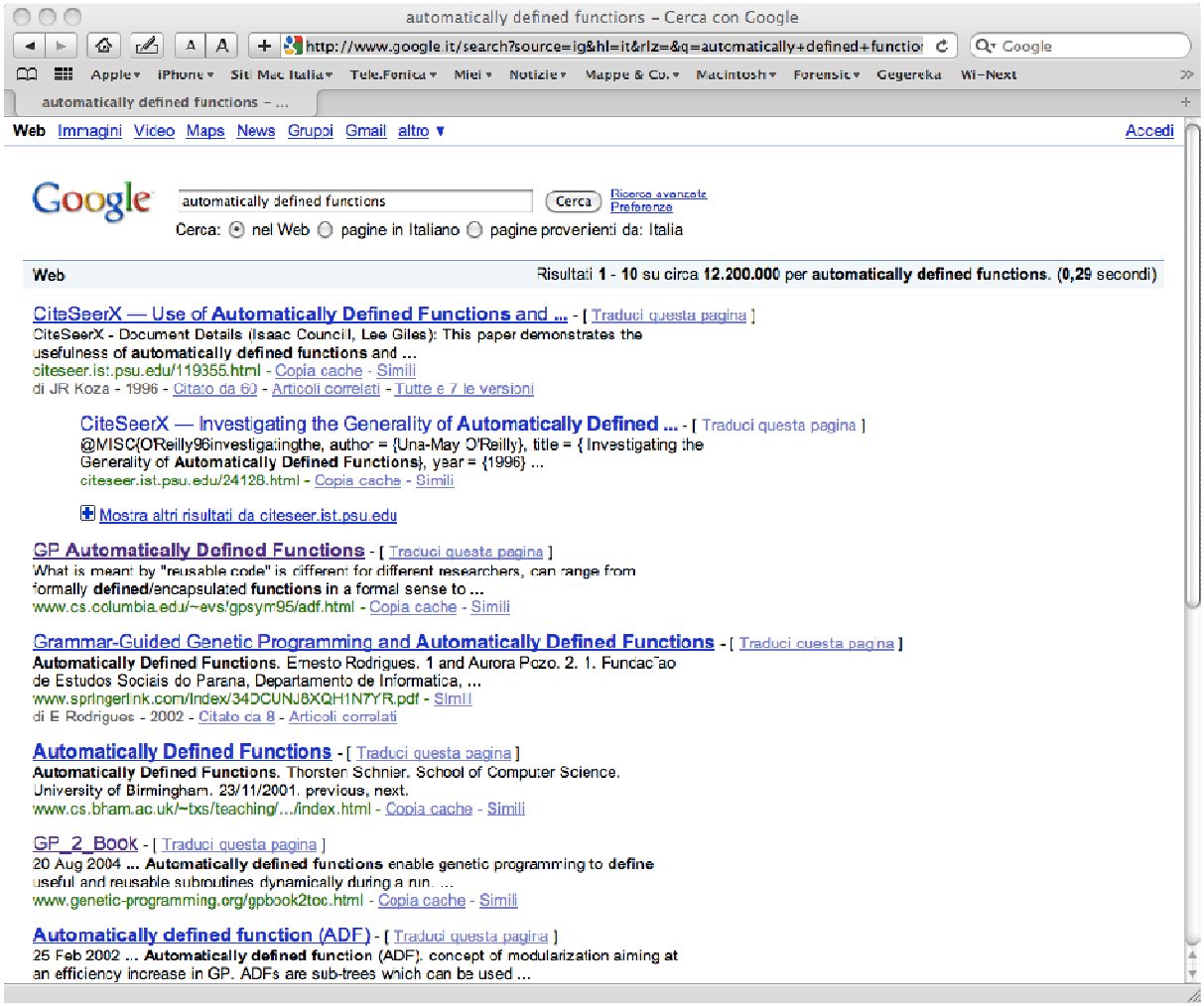

fig. 6

I seguenti due frammenti di codice richiamano, dunque, dei link trovati con la precedente ricerca.

<dict>
<key></key>
<string>http://ls11-www.cs.uni-dortmund.de/people/beyer/EA-glossary/node6.html</string>
<key>lastVisitedDate</key>
<string>215452340.2</string> > Tuesday 30 October 2007 04:52:20 PM <
<key>title</key>
<string>Automatically defined function (ADF)</string>
<key>visitCount</key>
<integer>1</integer>
</dict>

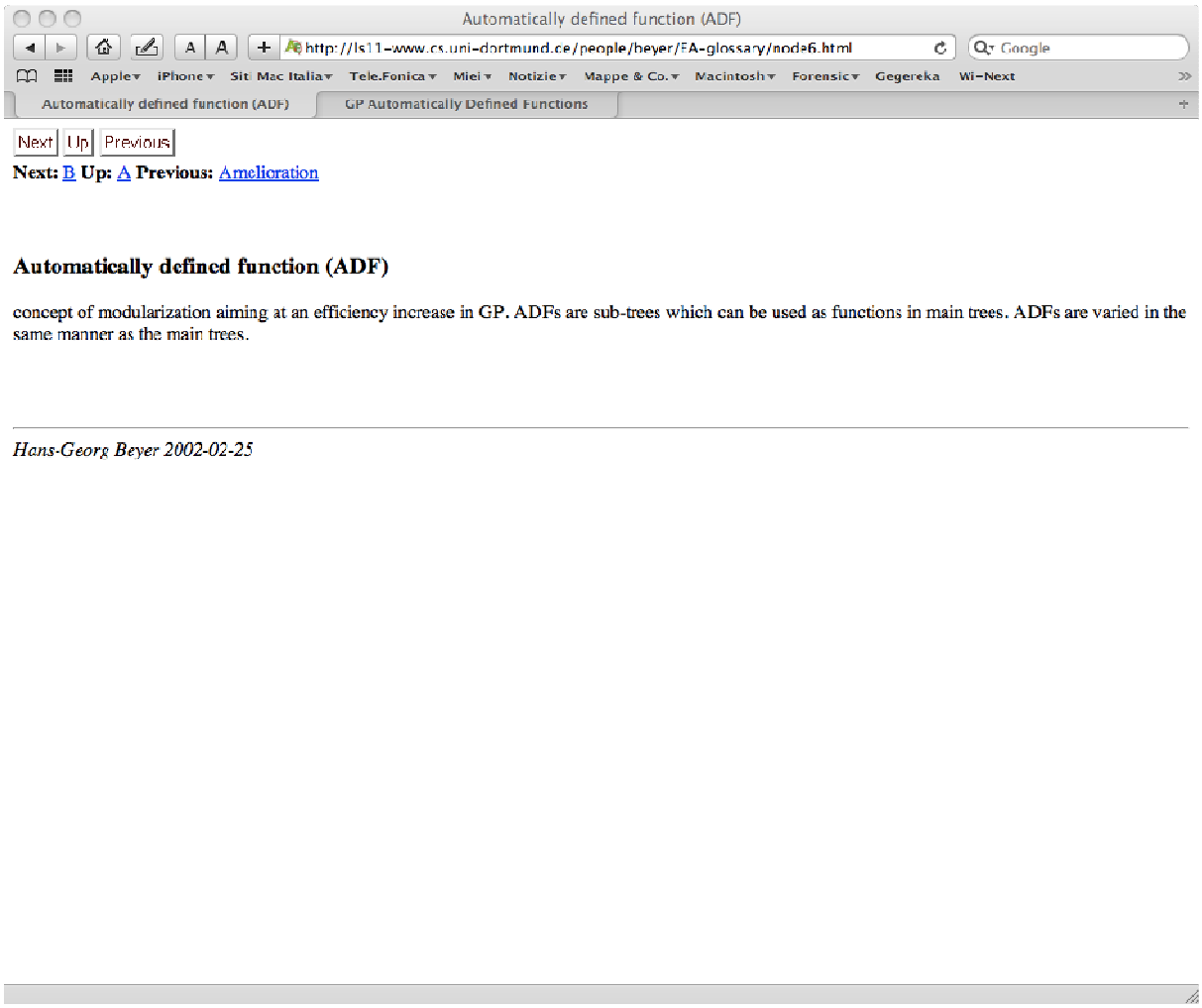

fig. 7

<dict>
<key></key>
<string>http://www.cs.columbia.edu/~evs/gpsym95/adf.html</string>
<key>lastVisitedDate</key>
<string>215452357.9</string> > Tuesday 30 October 2007 04:52:37 PM <
<key>title</key>
<string>GP Automatically Defined Functions</string>
<key>visitCount</key>
<integer>1</integer>
</dict>

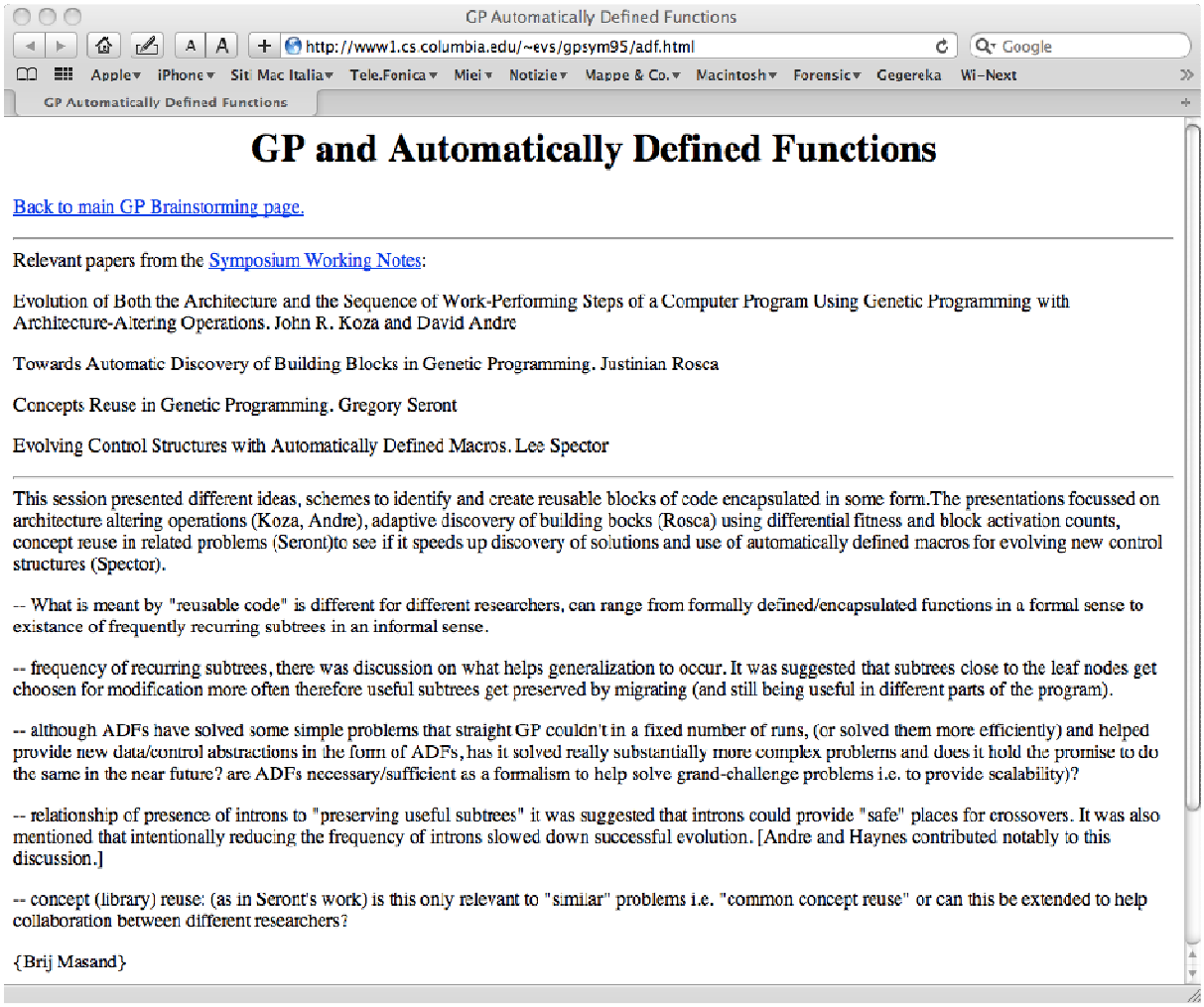

fig. 8

Continuando con la lettura dei frammenti del codice riscontriamo che è stata effettuata la stessa ricerca nelle immagini che come risultato ha dato, verosimilmente, la stessa pagina riportata in figura 9. Tutte le pagine successive sono ottenute utilizzando i suggerimenti proposti dalla ricerca.

<dict>
<key></key>
<string>http://images.google.it/images?source=ig&hl=it&rlz=&q=automatically%20defined%20functions&oe=UTF-8&um=1&ie=UTF-8&sa=N&tab=wi</string>
<key>lastVisitedDate</key>
<string>215452366.4</string> > Tuesday 30 October 2007 04:52:46 PM <
<key>title</key>
<string>automatically defined functions - Ricerca immagini Google</string>
<key>visitCount</key>
<integer>1</integer>
</dict>

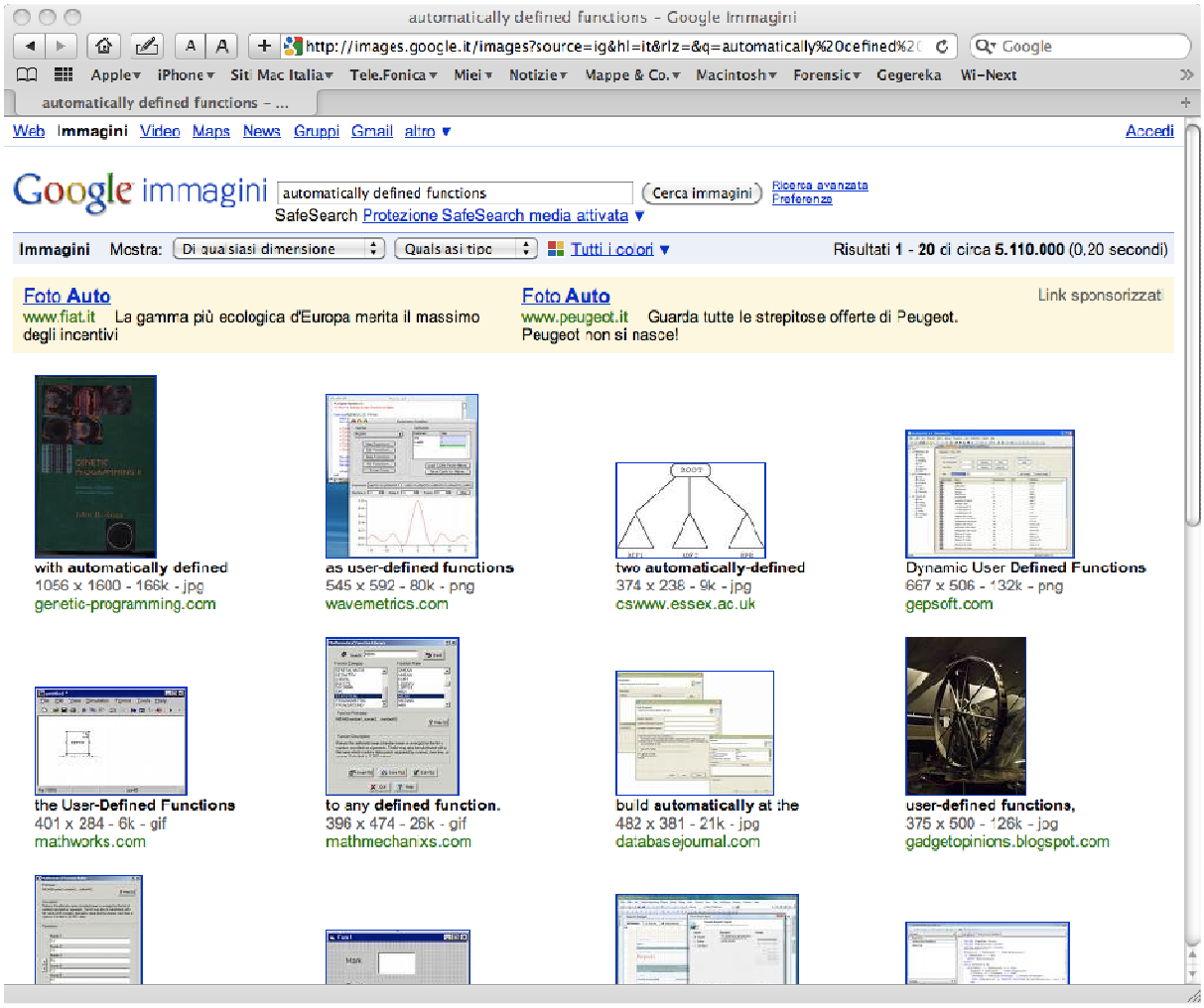

fig. 9

<dict>
<key></key>
<string>http://images.google.it/imgres?imgurl=http://nilsliberg.se/ksp/img/kscript_editor_1_03.jpg&imgrefurl=http://nilsliberg.se/ksp/&h=574&w=471&sz=72&hl=it&start=9&um=1&tbnid=V9vQyeJmzO6omM:&tbnh=134&tbnw=110&prev=/images%3Fq%3Dautomatically%2Bdefined%2Bfunctions%26svnum%3D10%26um%3D1%26hl%3Dit%26sa%3DN</string>
<key>lastVisitedDate</key>
<string>215452373.6</string> > Tuesday 30 October 2007 04:52:53 PM <
<key>title</key>
<string>Google. Risultato della ricerca di immagini per http://nilsliberg.se/ksp/img/kscript_editor_1_03.jpg</string>
<key>visitCount</key>
<integer>1</integer>
</dict>

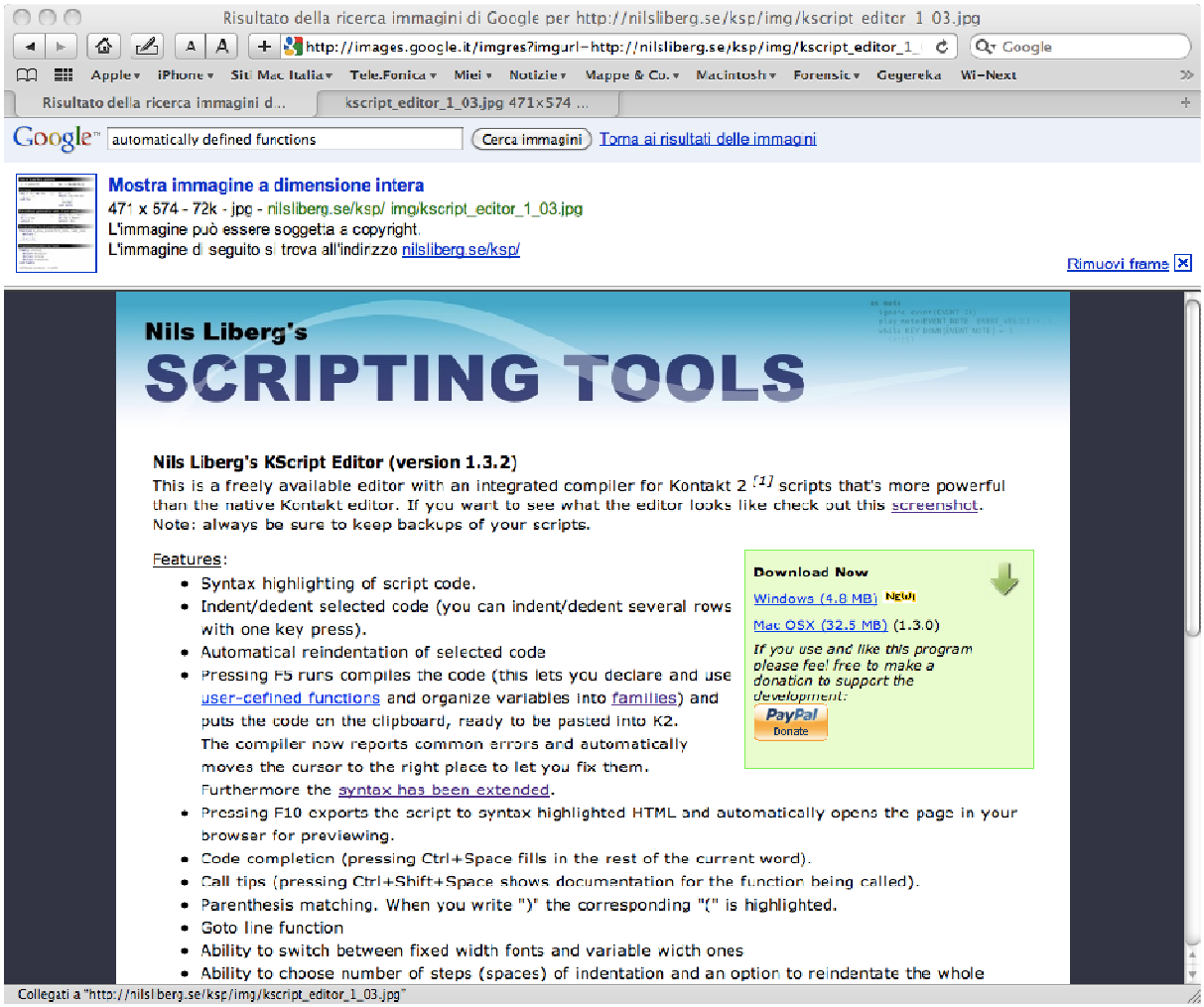

fig. 10

<dict>
<key></key>
<string>http://nilsliberg.se/ksp/img/kscript_editor_1_03.jpg</string>
<key>lastVisitedDate</key>
<string>215452380.8</string> > Tuesday 30 October 2007 04:53:00 PM <
<key>title</key>
<string>kscript_editor_1_03.jpg</string>
<key>visitCount</key>
<integer>1</integer>
</dict>

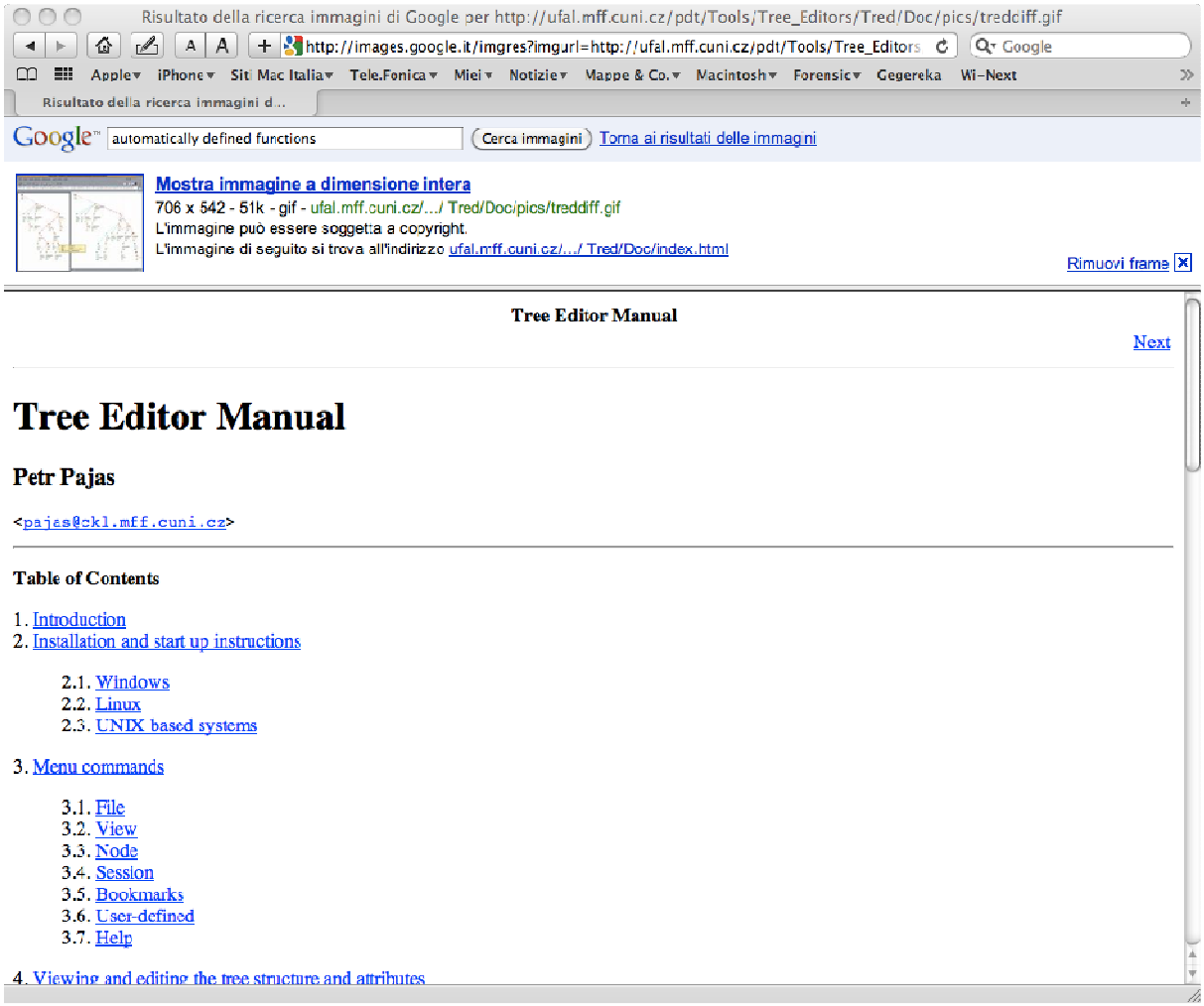

fig. 11

<dict>
<key></key>
<string>http://images.google.it/imgres?imgurl=http://ufal.mff.cuni.cz/pdt/Tools/Tree_Editors/Tred/Doc/pics/treddiff.gif
&imgrefurl=http://ufal.mff.cuni.cz/pdt/Tools/Tree_Editors/Tred/Doc/index.html&h=542&w=706&
sz=51&hl=it&start=16&um=1&tbnid=PyaAG_Nr9iO7dM:&tbnh=107&tbnw=140&
prev=/images%3Fq%3Dautomatically%2Bdefined%2Bfunctions%26svnum%3D10%26um%3D1%26hl%3Dit%26sa%
3DN</string>
<key>lastVisitedDate</key>
<string>215452405.1</string> > Tuesday 30 October 2007 04:53:25 PM <
<key>title</key>
<string>Google. Risultato della ricerca di immagini per
http://ufal.mff.cuni.cz/pdt/Tools/Tree_Editors/Tred/Doc/pics/treddiff.gif</string>
<key>visitCount</key>
<integer>1</integer>
</dict>

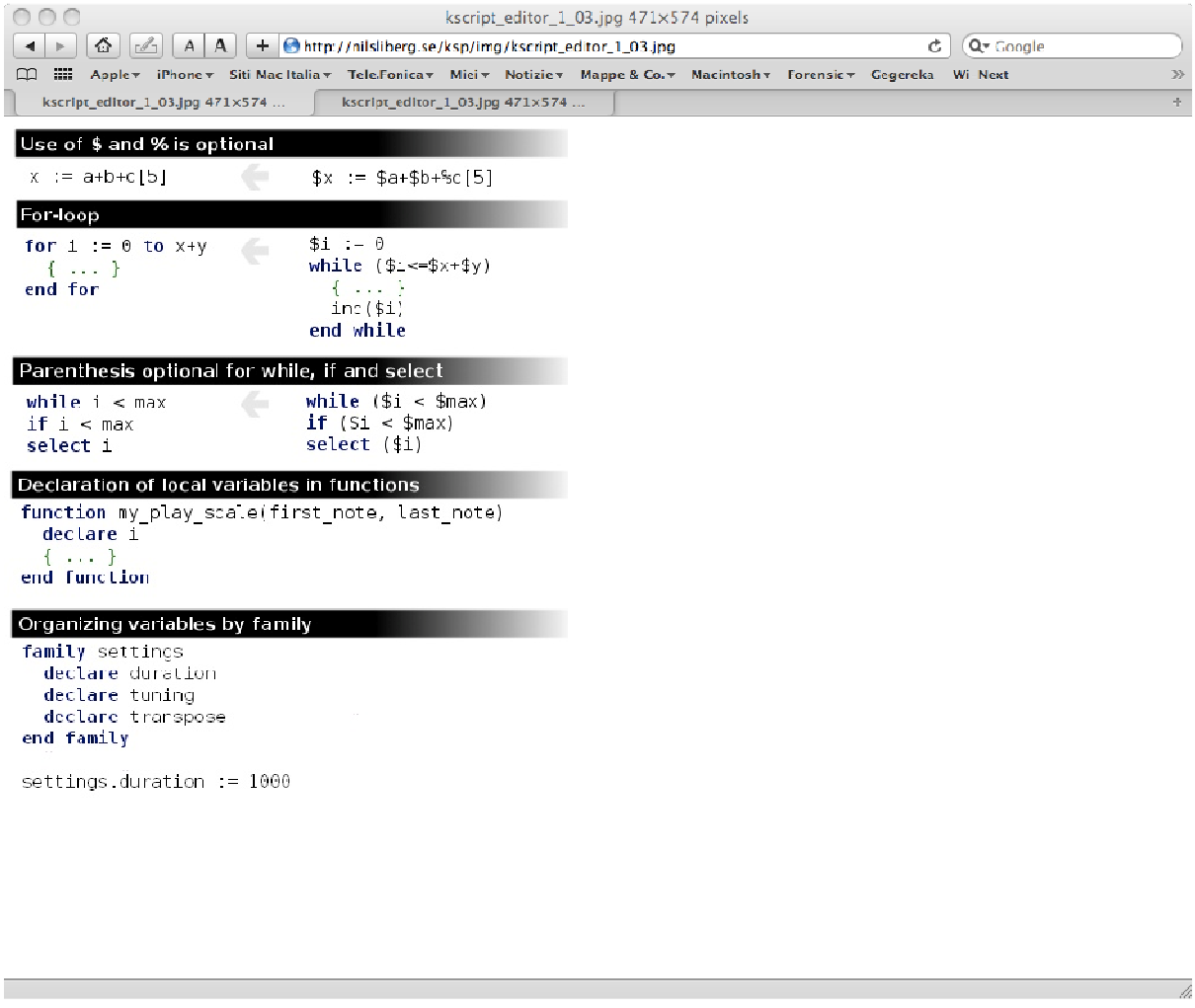

fig. 12

<dict>
<key></key>
<string>http://ufal.mff.cuni.cz/pdt/Tools/Tree_Editors/Tred/Doc/pics/treddiff.gif</string>
<key>lastVisitedDate</key>
<string>215452411.2</string> > Tuesday 30 October 2007 04:53:31 PM <
<key>title</key>
<string>treddiff.gif</string
<key>visitCount</key>
<integer>1</integer>
</dict>

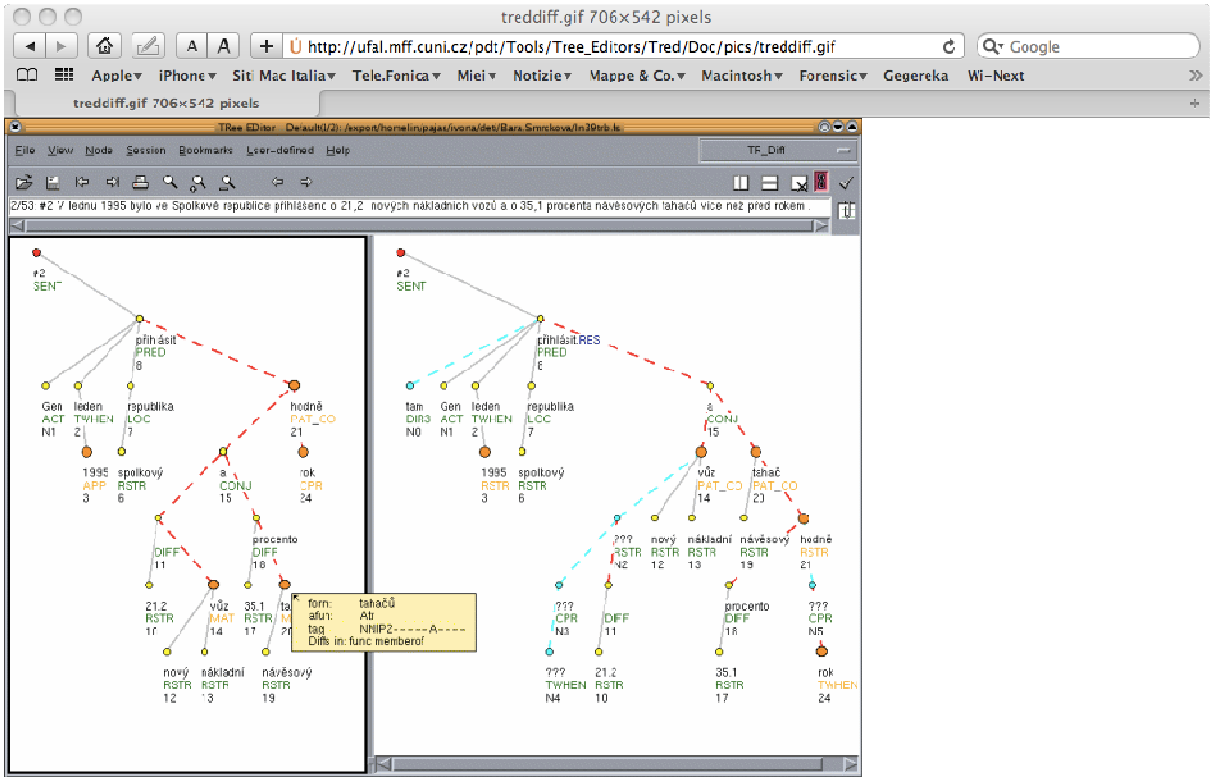

fig. 13

<dict>
<key></key>
<string>http://images.google.it/images?q=automatically+defined+functions&svnum=10&um=1&hl=it&start=18&sa=N&ndsp=18</string>
<key>lastVisitedDate</key>
<string>215452422.5</string> > Tuesday 30 October 2007 04:53:42 PM <
<string>automatically defined functions - Ricerca immagini Google</string>
<key>visitCount</key>
<integer>1</integer>
</dict>

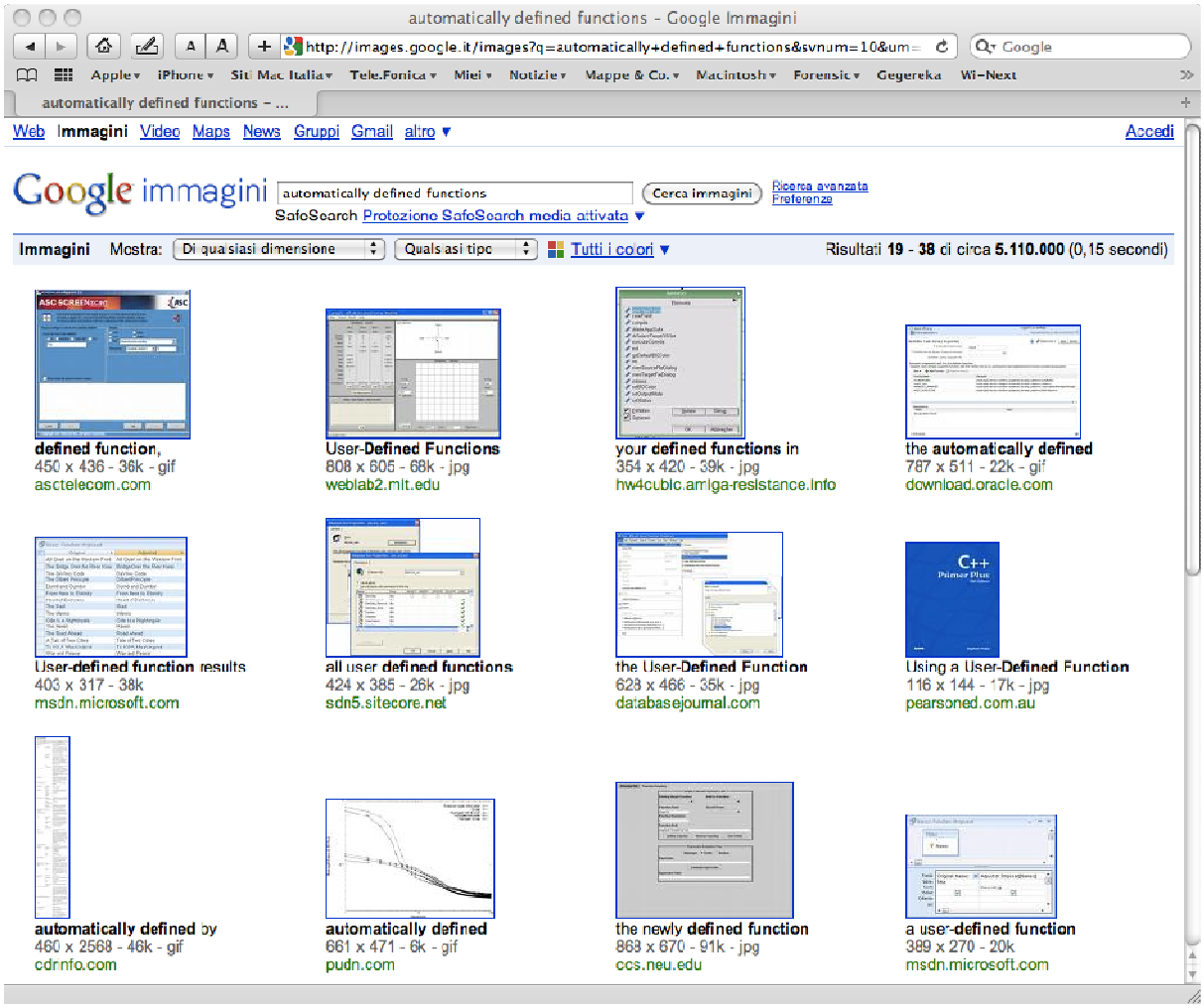

fig. 14

<dict>
<key></key>
<string>http://www.genetic-programming.org/gpbook2toc.html</string>
<key>lastVisitedDate</key>
<string>215452443.7</string> > Tuesday 30 October 2007 04:54:03 PM <
<key>title</key>
<string>GP_2_Book</string>
<key>visitCount</key>
<integer>1</integer>
</dict>

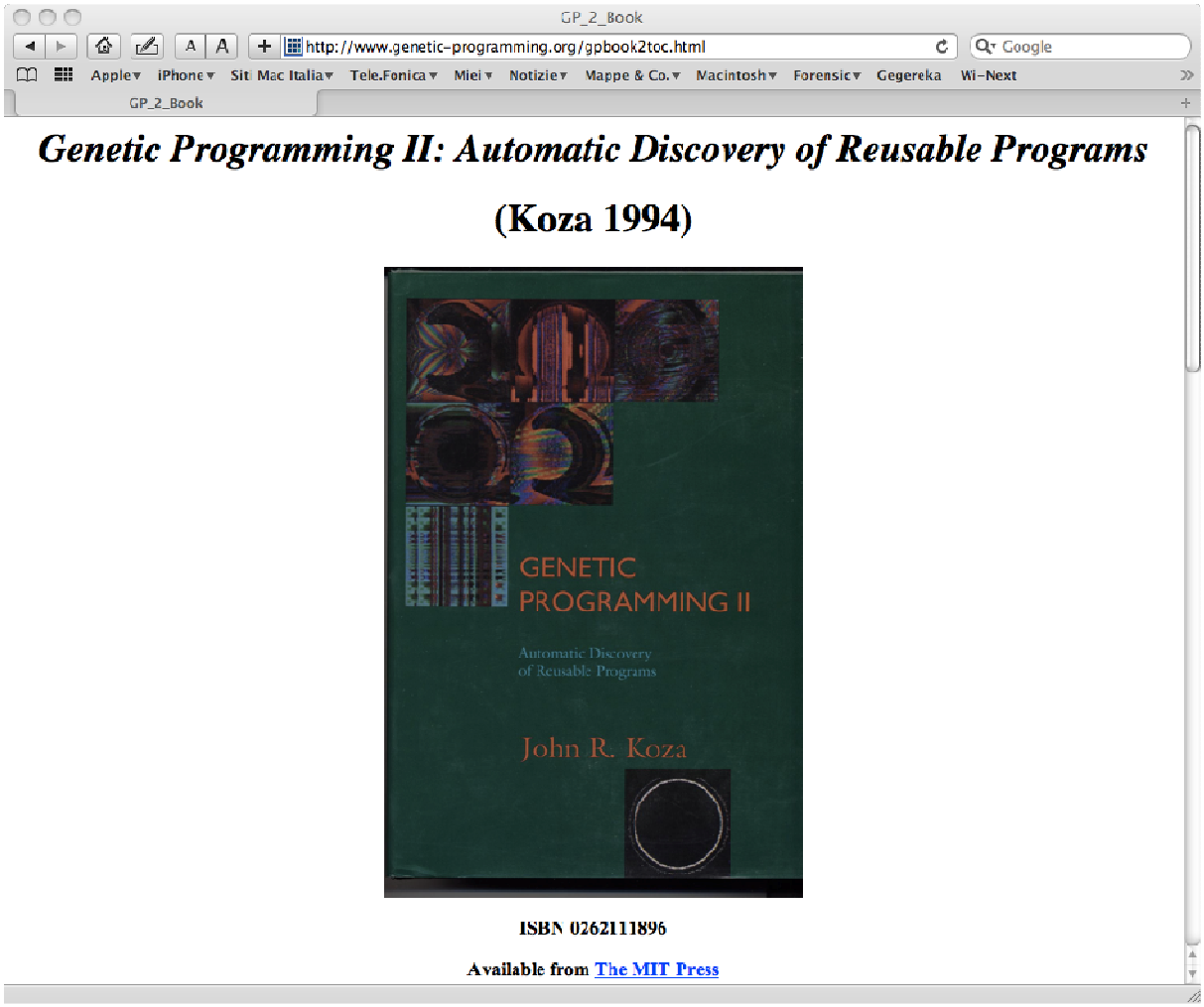

fig. 15

Anche in questa pagina è presente una ricerca che ha come chiave *"lisp programmazione genetica"* (figura 16).

<dict>
<key></key>
<string>http://www.google.it/search?source=ig&hl=it&rlz=&q=lisp+programmazione+genetica&btnG=Cerca+con+Google&meta=</string>
<key>lastVisitedDate</key>
<string>215452850.1</string> > Tuesday 30 October 2007 05:00:50 PM <
<key>title</key>
<string>lisp programmazione genetica - Cerca con Google</string>
<key>visitCount</key>
<integer>1</integer>
</dict>

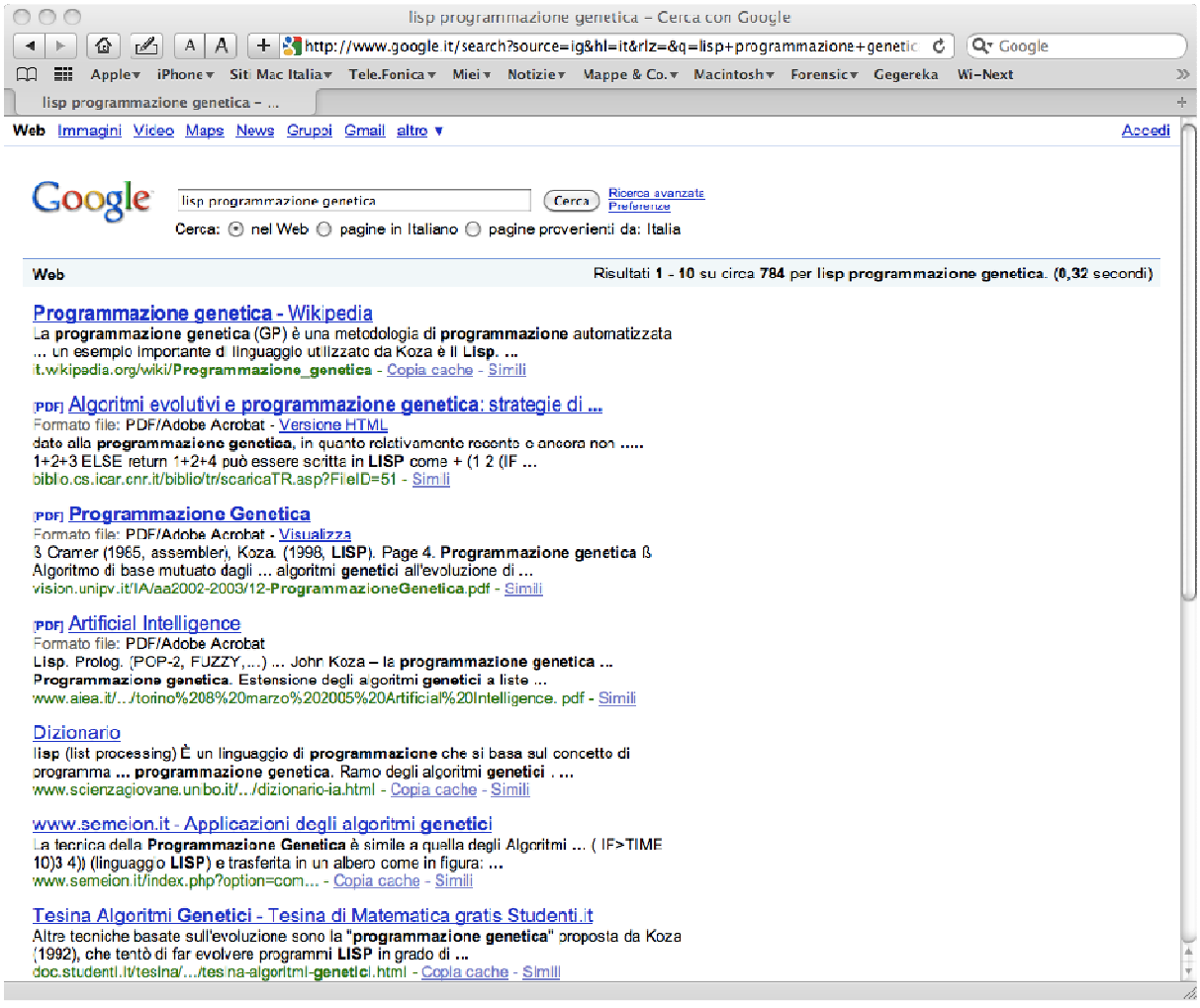

fig. 16

Apertura del primo dei link proposti.

<dict>
<key></key>
<string>http://it.wikipedia.org/wiki/Programmazione_genetica</string>
<key>lastVisitedDate</key>
<string>215452854.5</string> > Tuesday 30 October 2007 05:00:54 PM <
<key>title</key>
<string>Programmazione genetica - Wikipedia</string>
<key>visitCount</key>
<integer>1</integer>
</dict>

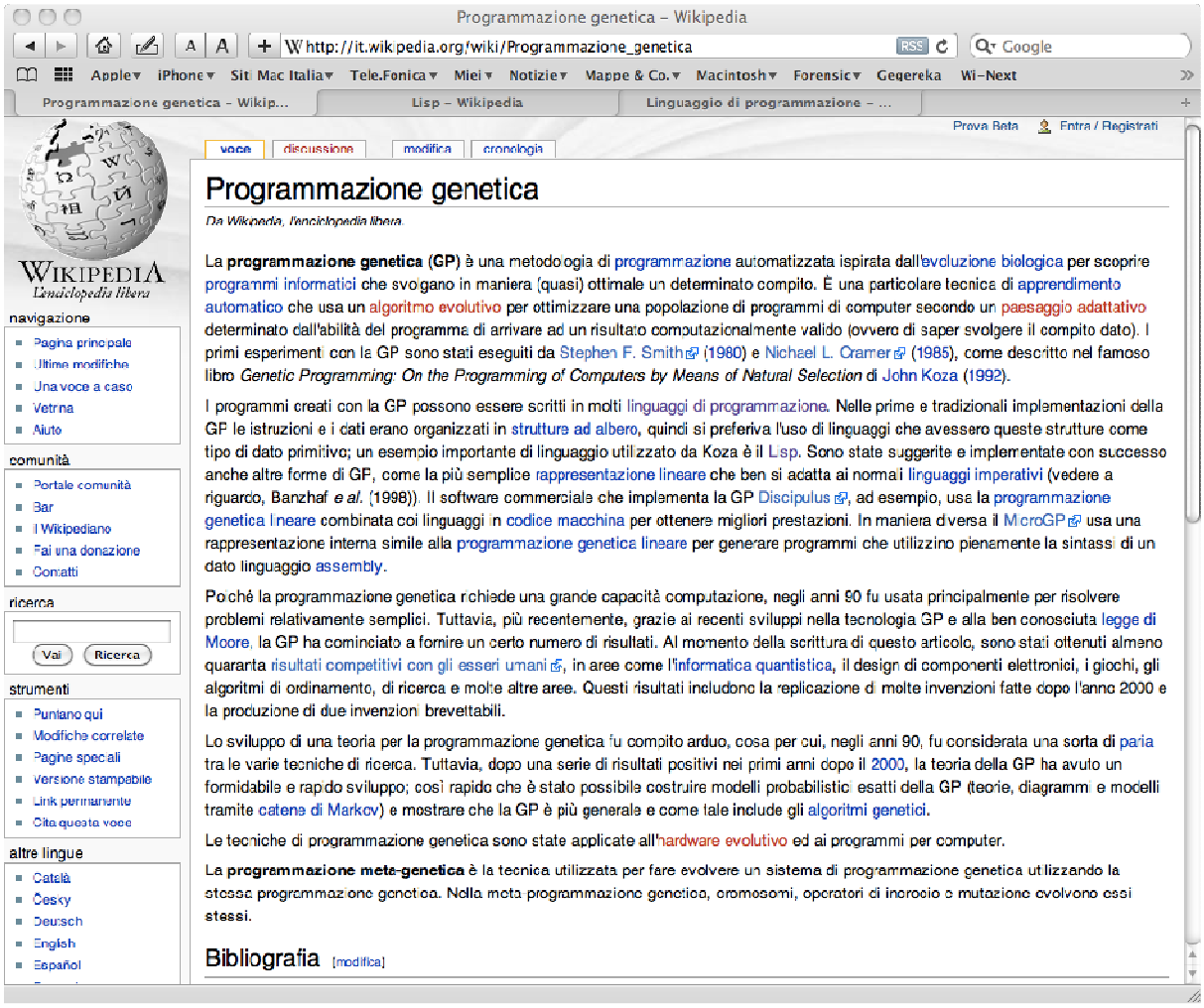

fig. 17

<dict>
<key></key>
<string>http://it.wikipedia.org/wiki/Lisp</string>
<key>lastVisitedDate</key>
<string>215452887.8</string> > Tuesday 30 October 2007 05:01:27 PM <
<key>title</key>
<string>Lisp - Wikipedia</string>
<key>visitCount</key>
<integer>1</integer>
</dict>

fig. 18

<dict>
<key></key>
<string>http://it.wikipedia.org/wiki/Linguaggio_di_programmazione</string>
<key>lastVisitedDate</key>
<string>215452951.6</string> > Tuesday 30 October 2007 05:02:31 PM <
<key>title</key>
<string>Linguaggio di programmazione - Wikipedia</string>
<key>visitCount</key>
<integer>1</integer>
</dict>

fig. 19

In conclusione possiamo affermare con assoluta certezza che tutte queste attività denotano una continua interazione con il computer e internet.

Adobe PDF Professional

Il software Adobe PDF Professional è stato utilizzato per leggere i files "*genetic-programming.pdf*" alle ore 16:54 e "*def._Tettamanzi_p._3-17.pdf*" alle ore 17:37, file legati alle ricerche mostrate in precedenza.

iTunes

L'analisi del file *"iTunes Music Library.xml"*, file che ha tutte le informazioni su su ogni brano che popola la libreria di iTunes, ha evidenziato che nel intervallo di tempo considerato c'è stata una interazione con l'applicativo relativamente allo "skip" di un brano; la parte di codice estratto dal file *"iTunes Music Library.xml"* (allegato F) riporta la stringa <key>Skip Date</key><date>2007-10-30T15:12:17Z</date> che indica che il file *"Andare.mp3"* è stato saltato alle ore 15:12:17; considerando che iTunes riporta la data in formato UTC, bisogna aggiungere un'ora ottenendo così le 16:12:17, stessa ora che rileviamo alla riga 2384 del file "*FILES 25-10_3-11-2007.xls"* (allegato A) ottenuto con Encase 6.8, ovvero 16:16

Name	File Ext	Description	Last Accessed	File Created	Last Written
Andare.mp3	mp3	File	30-10-07 16:12	29-10-06 00:12	29-10-06 00:12

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple Computer//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
	<key>Major Version</key><integer>1</integer>
	<key>Minor Version</key><integer>1</integer>
	<key>Application Version</key><string>7.4.2</string>
	<key>Features</key><integer>1</integer>
	<key>Show Content Ratings</key><true/>
	<key>Music Folder</key><string>file://localhost/Users/macbookpro/Music/iTunes/iTunes%20Music/</string>
	<key>Library Persistent ID</key><string>E3C6550B88CC5C89</string>
	<key>Tracks</key>
		<key>3036</key>
		<dict>
			<key>Track ID</key><integer>3036</integer>
			<key>Name</key><string>Andare</string>
			<key>Artist</key><string>Ludovico Einaudi</string>
			<key>Album</key><string>Divenire</string>
			<key>Genre</key><string>New Age</string>
			<key>Kind</key><string>Doc. audio MPEG</string>
			<key>Size</key><integer>10133339</integer>
			<key>Total Time</key><integer>422217</integer>
			<key>Year</key><integer>2006</integer>
			<key>Date Modified</key><date>2006-10-28T23:12:28Z</date>
			<key>Date Added</key><date>2007-10-23T19:47:01Z</date>
			<key>Bit Rate</key><integer>192</integer>
			<key>Sample Rate</key><integer>44100</integer>
			<key>Comments</key><string>R0X4</string>
			<key>Play Count</key><integer>2</integer>
			<key>Play Date</key><integer>3276102982</integer>
			<key>Play Date UTC</key><date>2007-10-24T19:36:22Z</date>
			<key>Skip Count</key><integer>1</integer>
			<key>Skip Date</key><date>2007-10-30T15:12:17Z</date>
			<key>Persistent ID</key><string>170DFB0D28261BF2</string>
			<key>Track Type</key><string>File</string>
<key>Location</key><string>file://localhost/Users/macbookpro/Music/iTunes/iTunes%20Music/Ludovico%20Einaudi/Divenire/Andare.mp3</string>
			<key>File Folder Count</key><integer>4</integer>
			<key>Library Folder Count</key><integer>1</integer>
		</dict>
</dict>
</plist>
```

Anche questa è traccia evidente di interazione umana con il computer.

Mail

Mail è il client di posta elettronica in dotazione con il sistema operativo Mac OS X. Alle ore 18:01 abbiamo rilevato che è stata scritta ed inviata una mail all'indirizzo baioletti@dipmat.unipg.itcon con allegato il file "Programmazione Genetica.doc" e indicizzata col nome 1969.emlx (Figura 20).

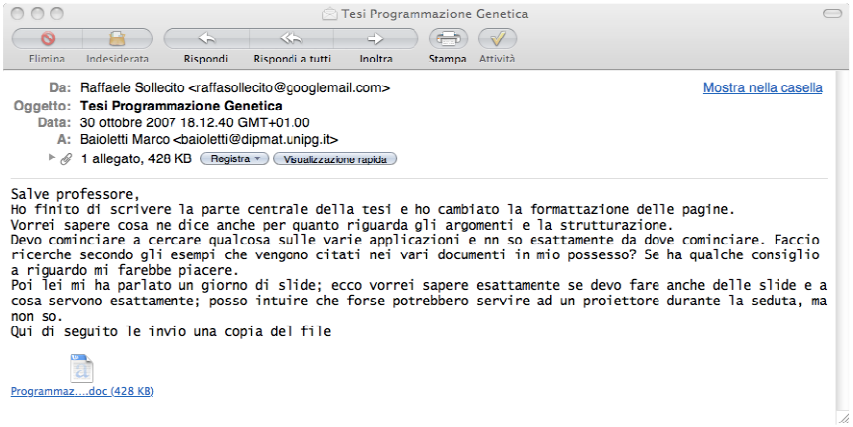

fig. 20

A questa mail ne è seguita una di risposta datata 30 ottobre 2007 ore 21:21:58 avente come mittente baioletti@dipmat.unipg.it indicizzata col nome 1970.emlx (Figura 21).

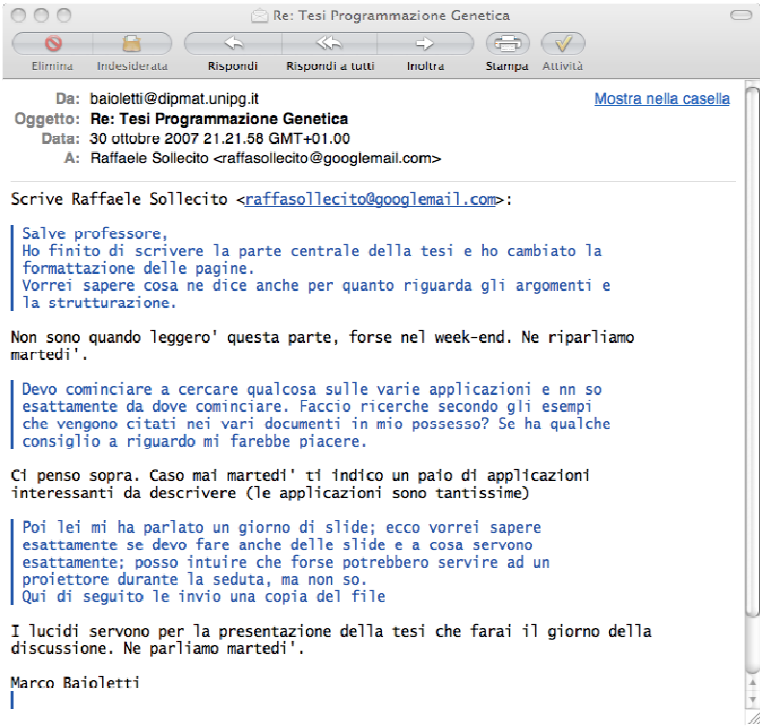

fig. 21

A conferma dell'invio della mail c'è l'esecuzione del file Mail "Sent.aiff" (riga 2689 del file *"FILES 25-10_3-11-2007.xls"* dell'allegato A), ovvero il suono che il software utilizza per indicare l'invio delle mail.

Relativamente al software Encase è importante fare la seguente considerazione: il software Encase, utilizzato dalla Polizia per analizzare il supporto magnetico in questione, è un ottimo strumento di ricerca e analisi, ma bisogna leggere il dato nella sua interezza, considerare cioè che il software rileva non solo l'ultimo accesso, ma anche la data di creazione e di ultima scrittura. Solo così si può risalire ad una informazione certa. Per i files, riportati in basso solo per esempio, infatti se ci si soffermasse solo alla data di ultimo accesso, si rileverebbe che al file 1969.emlx si è acceduto alle 22.24, mentre in realtà l'applicativo Mail del computer ci dice in modo inoppugnabile che questo file è stato creato e inviato dallo stesso alle ore 18.13 del giorno 30 ottobre, dato che corrisponde alla data di creazione anche per encase e riportata dal software nella seconda colonna. E' importante altresì evidenziare che in questo caso e cioè allorquando è il computer a generare il file è possibile anche con il software encase rilevare la data di creazione.
Quando invece vi è un semplice accesso al file sia da parte dell'utente, che dall'esterno attraverso la rete internet, il software encase fornisce solo la data di ultimo accesso, sovrascrivendo in automatico l'accesso precedente. In questo modo si perde ogni dato storico su quel file. Queste informazioni sul file di tipo storico si possono ottenere solo analizzando i files di log qualora presenti. Questo discorso vale per analogia sulla interpretazione del file 1970.emlx.

Name	File Ext	Description	Last Accessed	File Created	Last Written
1969.emlx	emlx	File	30-10-07 22:24	30-10-07 18:13	30-10-07 22:24
1970.emlx	emlx	File	05-11-07 13:12	30-10-07 22:24	05-11-07 13:12

Per chiarire ulteriormente il funzionamento di Encase, prendiamo in esame il file video *"(Divx-Ita) Stardust Ok.avi"*. Se cerchiamo informazioni su questo file troviamo sul file generato da Encase che l'ultimo accesso risale alle 02:47 del 06 Novembre 2007, mentre dal log di aMule leggiamo che il download è iniziato alle 17:03:42 del 01 novembre 2007 e terminato alle 19:19:04 del 01 novembre. Il film in questione è stato visionato con il lettore multimediale VLC successivamente alla visione de "Il favoloso mondo di Amelie"; questo può significare:

- il file è stato visto il 06 Novembre alle ore 02:47;
- il giorno 06 Novembre ha acceduto al file uno dei software P2P;
- il file è stato visto in un altro momento compreso tra la data di creazione e quella di ultimo accesso.

Queste considerazioni portano ad affermare che parte dei dati su cui abbiamo lavorato possono presentare delle alterazioni di data di ultimo accesso, generate dall'esterno (software P2P) o da una interazione umana.

Riteniamo utile infine far presente che il giorno 30 ottobre 2007 era in regime di ora solare ovvero il sole è sorto alle ore 6:11 ed è tramontato alle ore 17:36. (vedi allegato G).

-2 DALLE ORE 22.00 ALLE ORE 5.00 DEI GIORNI 01-02 NOVEMBRE 2007

Analisi dei dati relativa alle attività svolte dalle ore 22:00 del giorno 01 Novembre 2007 alle ore 5:00 del 02 Novembre

Analizzando i tabulati forniti dall'azienda fornitrice del servizio di connettività Fastweb SPA contenenti tutte le sessioni generate dal computer in questione verso il mondo internet, abbiamo rilevato un notevole traffico costituito principalmente da P2P (PeerToPeer); è noto infatti che il computer fosse sempre collegato e connesso alla rete per permettere a software come Azureus e aMule di continuare con il download/upload dei files selezionati. E' tuttavia presente, seppure in quantità minore, un traffico "www-http" riconoscibile dalla porta di destinazione 80/tcp (allegato M scaricabile dal link *http://www.iana.org/assignments/port-numbers*). Parte traffico web è di tipo automatico, auto-generato a intervalli regolari dal browser Firefox verso IP riconducibili a Google e Mozilla; ma abbiamo rilevato oltre a questo traffico che alle ore 00:58:50 c'è traffico con l'IP 17.112.152.32 la cui traduzione punta all'home page www.apple.com. (Tracciati fastweb Allegato L). Ciò significa a nostro avviso che c'è stato un accesso al sito internazionale della Apple all'ora indicata da parte di un utente. Quindi alle ore 00.58 del giorno 02 novembre 2007 vi è stata una interazione umana con il computer.

-3 DALLE ORE 11.30 ALLE ORE 12.30 DEL GIORNO 02 NOVEMBRE 2007

Analisi dei dati relativa alle attività svolte il giorno 02 Novembre 2007 dalle ore 11:30 alle ore 12:30

Anche per il periodo in questione abbiamo usato il file History.plist di Safari per individuare segni di interazione con il computer. Nelle righe di codice estratte dal file indicato, individuiamo richieste al sito mail.google.it e facebook.com.

<dict>
<key></key>
<string>http://mail.google.com/mail/?attid=0.2&disp=inline&view=att&th=115f6b02d664c666</string>
<key>lastVisitedDate</key>
<string>215695205.9</string> > Friday 02 November 2007 12:20:05 PM <
<key>title</key>
<string>Gmail - IMGP3026.JPG</string>
<key>visitCount</key>
<integer>1</integer>
</dict>

<dict>
<key></key>
<string>http://mail.google.com/mail/?attid=0.1&disp=vah&view=att&th=115fb04cacce172e</string>
<key>lastVisitedDate</key>
<string>215695336.0</string> > Friday 02 November 2007 12:22:16 PM <
<key>visitCount</key>
<integer>1</integer>
</dict>

<dict>
<key></key>
<string>http://washington.facebook.com/profile.php?id=10723761&ref=ts</string>
<key>lastVisitedDate</key>
<string>215759320.0</string> > Friday 02 November 2007 12:22:16 PM <
<key>title</key>
<string>Facebook | David Johnsrud</string>
<key>visitCount</key>
<integer>1</integer>
</dict>

Se inoltre guardiamo le righe 4353-4380 del file "*FILES 25-10_3-11-2007.xls*" (allegato A) del tracciato EnCase 6.8, notiamo che alle 12:15 c'è una ripresa delle attività (avviata manualmente) del computer che mette in evidenza interazione su file multimediali condivisi e già scaricati in precedenza, operazioni automatiche generate dalla ripresa delle attività.

Anche analizzando l'applicazione Mail abbiamo trovato un richiamo ai seguenti due file che contengono i messaggi che l'applicativo utilizza per dialogare con chi interagisce con il computer:

MacOS HD\System\Library\Frameworks\Message.framework\Versions\B\Resources\Italian.lproj\Message.strings

MacOS HD\System\Library\Frameworks\AppKit.framework\Versions\C\Resources\Italian.lproj\Delayed.strings

Quindi possiamo affermare che anche in questo spazio temporale ci sono state chiare interazioni umane con il computer dalle ore 12.15, alle ore 12.26.

-4 DALLE ORE 22.00 ALLE ORE 13.30 DEI GIORNI 05-06 NOVEMBRE 2007

Analisi dei dati relativa alle attività svolte dalle ore 22:00 del giorno 05 Novembre 2007 alle ore 13:30 del 06 Novembre

Per quest'ultimo intervallo di tempo abbiamo ricostruito le attività sul computer dividendole in una fase in cui si presume l'utilizzo del computer da parte del proprietario Raffaele Sollecito ed una successiva in cui il computer è stato utlilizzato da persona a noi sconosciuta, visto che dagli Atti processuali Sollecito non poteva essere presente in casa in quello spazio temporale. L'utilizzo del computer da parte del proprietario a nostro avviso si è concluso alle ore 20.00 del giorno 05 novembre 2007 con l'utilizzo del programma Skype.

L'attività umana con il computer riprende certamente alle ore **22.05** in modo intenso e più o meno continuativo con l'accesso al browser **Safari** e proseguendo con l'accesso all'applicativo **Messenger, Skype, Adobe Golive CS2 (ore 22.10**), l'apertura dell'applicativo **Mail (ore 23.07), Finder (00.58), Itunes, Firefox** come illustrato nella seguente tabella:

Adobe GoLive CS2.app	05-11-07 22:10
Partenza dello ScreenSaver	05-11-07 22:20
Mail.app	05-11-07 23:07
AddressBook.data	05-11-07 23:07
Finder.app	06-11-07 00:58
iTunes.app	06-11-07 00:58
Firefox.app	06-11-07 01:11

Riprende alle ore **09.07** con un nuovo accesso al browser **Safari e al browser Firefox con l'apertura** attraverso quest'ultimo della pagina Web **http: //www.ansa.it/main/notizie/awnplus/topnews/topnews.html,** che portava come titolo **"Inglese uccisa: eseguiti dei fermi"** e descrizione **"individuate le persone coinvolte alle ore 11 conferenza stampa".**

<rss version="2.0">
<channel>
  <title>ANSA.it - Top News</title>
  <link>http://www.ansa.it/main/notizie/awnplus/topnews/topnews.html</link>
  <description>Updated every day - FOR PERSONAL USE ONLY</description>
  <language>it</language>
  <copyright>Copyright: (C) ANSA, http://www.ansa.it/mainhtml/disclaimer.html</copyright>

<item>
<title>Inglese uccisa: eseguiti dei fermi</title>
<description>Individuate le persone coinvolte, alle 11 conferenza stampa</description>
<link>http://www.ansa.it/site/notizie/awnplus/topnews/news/2007-11-06_106130844.html</link>
<copyright>Copyright ANSA Tutti i diritti riservati</copyright>
<pubDate>2007-11-06 09:20</pubDate>

</item>

<item>
<title>Scioperi:verso stop trasporti il 30</title>
<description>Sindacati programmano stop di 8 ore contro la Finanziaria</description>
<link>http://www.ansa.it/site/notizie/awnplus/topnews/news/2007-11-06_106130718.html</link>
<copyright>Copyright ANSA Tutti i diritti riservati</copyright>
<pubDate>2007-11-06 09:09</pubDate>
</item>

<item>
<title>Terremoti: forte scossa in Messico</title>
<description>Sisma di magnitudo 5,6 Richter,epicentro in regione Acapulco</description>
<link>http://www.ansa.it/site/notizie/awnplus/topnews/news/2007-11-06_106130637.html</link>
<copyright>Copyright ANSA Tutti i diritti riservati</copyright>
<pubDate>2007-11-06 09:00</pubDate>
</item>

<item>
<title>Inglese uccisa: persone in Questura</title>
<description>Sul posto il pm che segue il caso, massimo riserbo</description>
<link>http://www.ansa.it/site/notizie/awnplus/topnews/news/2007-11-06_106130583.html</link>
<copyright>Copyright ANSA Tutti i diritti riservati</copyright>
<pubDate>2007-11-06 08:47</pubDate>
</item>

<item>
<title>E' morto Enzo Biagi</title>
<description>Il giornalista era ricoverato da dieci giorni a Milano</description>
<link>http://www.ansa.it/site/notizie/awnplus/topnews/news/2007-11-06_106130489.html</link>
<copyright>Copyright ANSA Tutti i diritti riservati</copyright>
<pubDate>2007-11-06 08:34</pubDate>
</item>

<item>
<title>Terrorismo:blitz del Ros,20 arresti</title>
<description>Stranieri avrebbero reclutato kamikaze verso l'Iraq</description>
<link>http://www.ansa.it/site/notizie/awnplus/topnews/news/2007-11-06_106130260.html</link>
<copyright>Copyright ANSA Tutti i diritti riservati</copyright>
<pubDate>2007-11-06 07:53</pubDate>
</item>

<item>
<title>Mafia: Lo Piccolo, analisi pizzini</title>
<description>Trovati in villetta dove e'stato arrestato"erede" Provenzano</description>
<link>http://www.ansa.it/site/notizie/awnplus/topnews/news/2007-11-06_106130235.html</link>
<copyright>Copyright ANSA Tutti i diritti riservati</copyright>
<pubDate>2007-11-06 07:39</pubDate>
</item>

<item>
<title>Borsa Tokyo chiude in ribasso</title>
<description>Indice Nikkei a -0,12%, euro si rafforza su dollaro e yen</description>
<link>http://www.ansa.it/site/notizie/awnplus/topnews/news/2007-11-06_106130204.html</link>
<copyright>Copyright ANSA Tutti i diritti riservati</copyright>
<pubDate>2007-11-06 07:22</pubDate>
</item>
</channel>
</rss>

Nello specifico all'apertura di Mail il sistema contatta immediatamente i server per il download (scarico) dei nuovi messaggi e, terminata l'operazione, riproduce un suono; come risulta dal file delle ore 23.07 1987.emlx (riga 62249 del file FILES 3-11_6-11-2007.xls) seguito dal suono di notifica "New Mail.aiff" (riga 62245 del file FILES 3-11_6-11-2007.xls).

Il file AddressBook.data è automaticamente richiamato da mail per tutte le operazioni che richiedono auto completamento degli indirizzi di posta elettronica o verifica della presenza di un mittente nella propria rubrica.

L'applicazione Finder.app si attiva quando si "clicca" sull'icona che richiama il sistema operativo (icona bicolore azzurra/celeste rappresentante due volti uno posto frontalmente e l'altro di profilo). Ricordiamo che il Finder è per i sistemi operativi Apple l'equivalente del processo chiamato explorer.exe dei sistemi Microsoft e racchiude tutte le operazioni che normalmente un utente esegue sul desktop o sulle cartelle in esso contenute, o per individuare un file o un'applicazione da eseguire, come nel nostro caso potrebbe essere iTunes.app.

Ultima applicazione eseguita/richiamata in ordine di tempo e Firefox.app.

Possiamo asserire inoltre che alle 10:20:57 del 6 Novembre il computer viene messo in ibernazione per essere riattivato alle 13:27:36 e quindi definitivamente regolarmente spento alle 13:35 circa (allegato H).

In fede	In fede
Dott. Michele Gigli	Dott. Antonio d'Ambrosio

Bari 18 settembre 2009

Allegato A

FILES 25-10_3-11-2007.xls

FILES 3-11_6-11-2007.xls

Allegato B

Safari History commentata e datata.pdf

Allegato C

Pagine web 30-10 dalle 12 alle 17

Allegato D

Files Mail

Allegato E

aMule

Allegato F

iTunes

Allegato G

Ora legale 30 ottobre

Allegato H

Sospensione del 6 novembre

Allegato I

Attività 2 Novembre 2007

Allegato L

Porte 80 traffico Fastweb

Allegato M

Porte Internet