

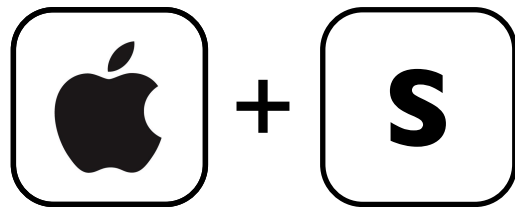
MAC OS X FORENSIC

Università degli Studi di Perugia

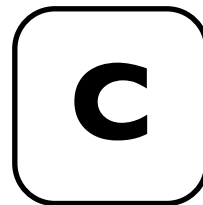


di
Luca Mariani e Andrea Nardinocchi

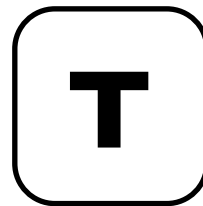
- Single user mode



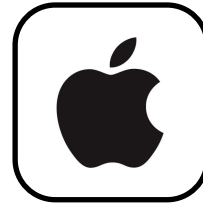
- ● Distribuzione Live Personalizzata



- ● Avviare in Target Disk Mode



SINGLE USER MODE



+

S

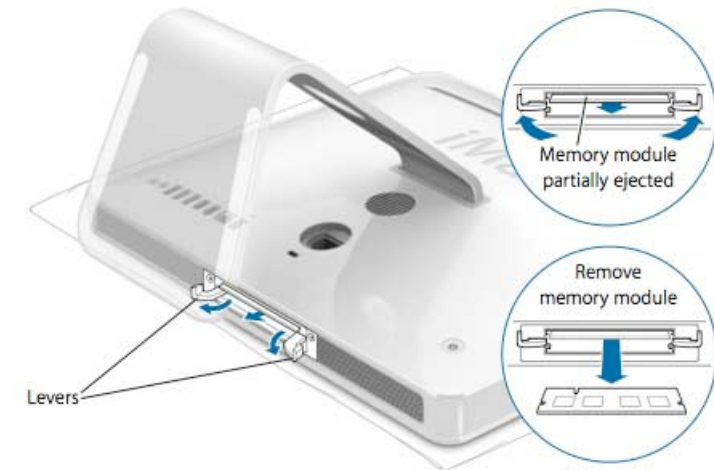
Modificare le password degli account presenti nel sistema:

```
Cerberus: ~ # mount -uw /  
Cerberus: ~ # passwd root  
New password for root:  
Repeat password for root:  
Cerberus: ~ # sync  
Cerberus: ~ # reboot
```

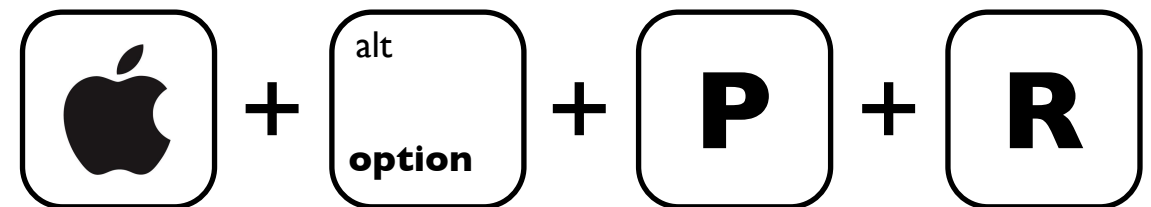
```
Cerberus: ~ # mount -uw /  
Cerberus: ~ # rm /var/db/.AppleSetupDone  
Cerberus: ~ # reboot
```

RESET FIRMWARE PASSWORD

Rimuovere almeno un modulo RAM in modo da cambiare il quantitativo di memoria presente nella macchina.



Avviare la macchina e resettare la **PRAM**.



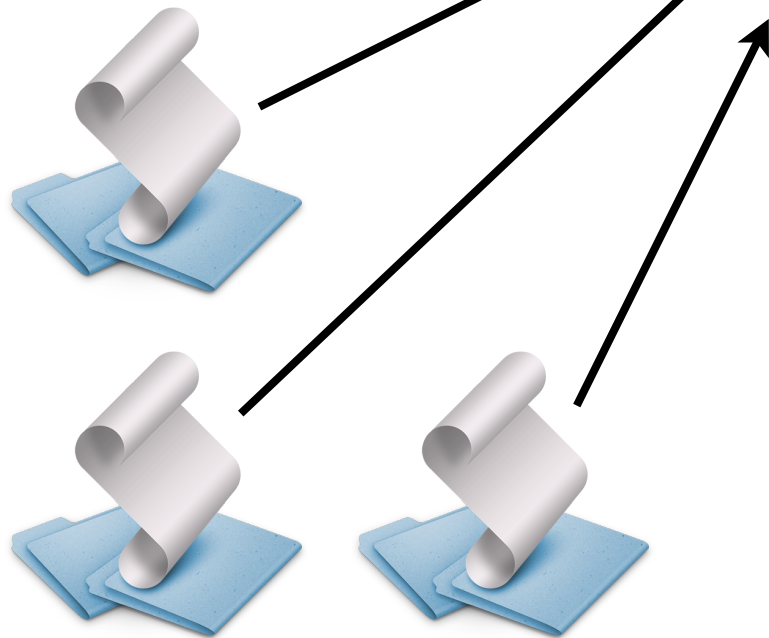
Spegnere la macchina e reinserire il modulo rimosso.

PARAMETER RAM:
Memoria non volatile in cui il sistema memorizza una suite di informazioni molto importanti tra cui la time zone, il volume delle casse e la password del firmware.

CUSTOM LIVE DISTRIBUTION



the Sleuth Kit
corredato eventualmente
dalla sua interfaccia
Autopsy



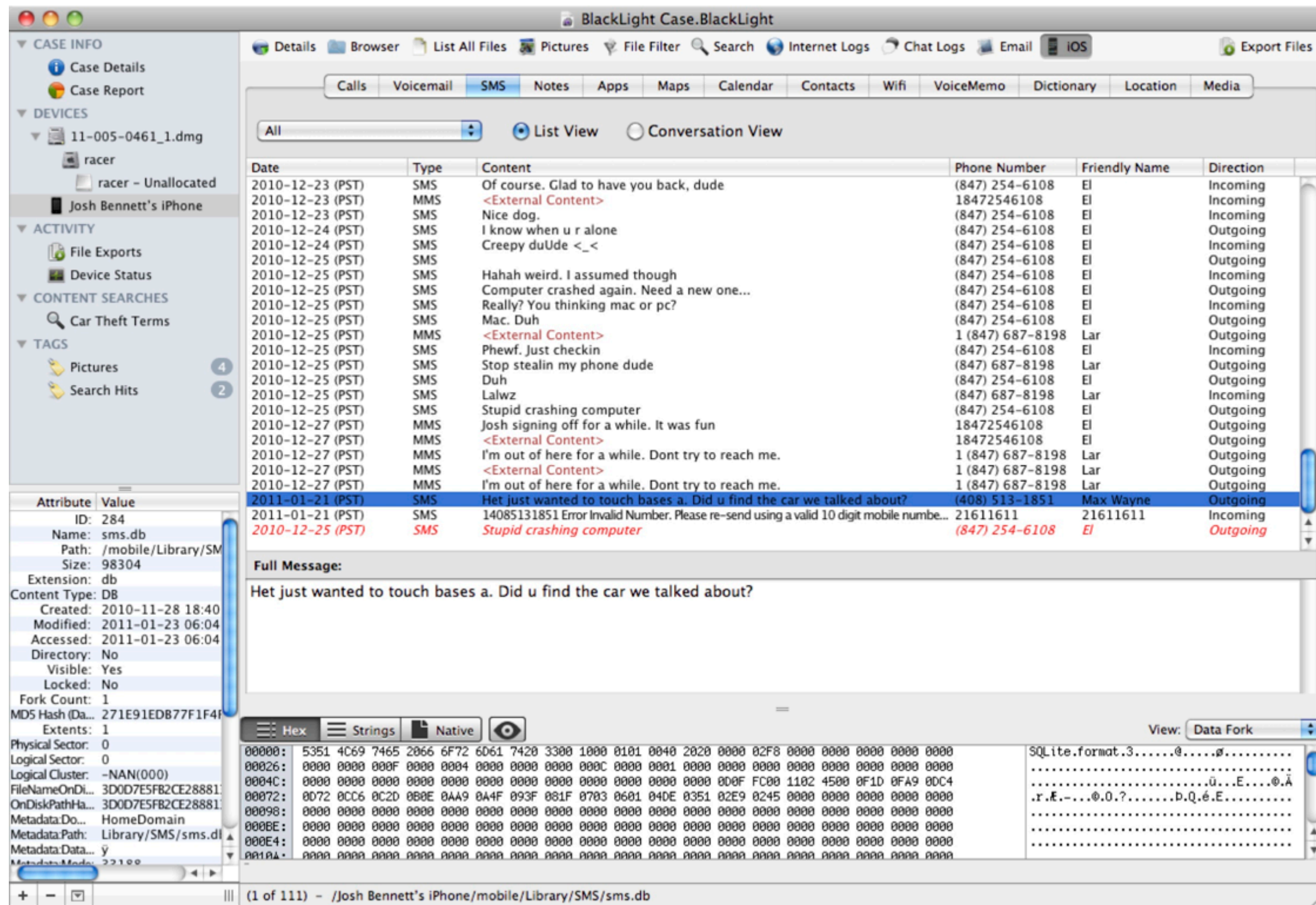
Altri script creati ad-hoc



Luca Mariani e Andrea Nardinocchi

BLACKLIGHT

prezzo: 2500\$



The screenshot displays the BlackLight Case.BlackLight application interface. The left sidebar shows the 'CASE INFO' section with 'Case Details' and 'Case Report' options. Below this, the 'DEVICES' section lists '11-005-0461_1.dmg' and 'racer'. The 'ACTIVITY' section includes 'File Exports' and 'Device Status'. The 'CONTENT SEARCHES' section shows 'Car Theft Terms'. The 'TAGS' section lists 'Pictures' (4 items) and 'Search Hits' (2 items).

The main window shows a list of SMS messages. The selected message is from 'Max Wayne' (phone number 408 513-1851) with the content 'Het just wanted to touch bases a. Did u find the car we talked about?'. The message is dated 2011-01-21 (PST) and is outgoing.

The bottom section shows the 'Full Message' details, including the date, time, and content. The 'Hex' view is also visible, showing the raw data of the message.

Date	Type	Content	Phone Number	Friendly Name	Direction
2010-12-23 (PST)	SMS	Of course. Glad to have you back, dude	(847) 254-6108	El	Incoming
2010-12-23 (PST)	MMS	<External Content>	18472546108	El	Incoming
2010-12-23 (PST)	SMS	Nice dog.	(847) 254-6108	El	Incoming
2010-12-24 (PST)	SMS	I know when u r alone	(847) 254-6108	El	Outgoing
2010-12-24 (PST)	SMS	Creepy duUde <_<	(847) 254-6108	El	Incoming
2010-12-25 (PST)	SMS		(847) 254-6108	El	Outgoing
2010-12-25 (PST)	SMS	Hahah weird. I assumed though	(847) 254-6108	El	Incoming
2010-12-25 (PST)	SMS	Computer crashed again. Need a new one...	(847) 254-6108	El	Outgoing
2010-12-25 (PST)	SMS	Really? You thinking mac or pc?	(847) 254-6108	El	Incoming
2010-12-25 (PST)	SMS	Mac. Duh	(847) 254-6108	El	Outgoing
2010-12-25 (PST)	MMS	<External Content>	1 (847) 687-8198	Lar	Outgoing
2010-12-25 (PST)	SMS	Phewf. Just checkin	(847) 254-6108	El	Incoming
2010-12-25 (PST)	SMS	Stop stealin my phone dude	(847) 687-8198	Lar	Outgoing
2010-12-25 (PST)	SMS	Duh	(847) 254-6108	El	Outgoing
2010-12-25 (PST)	SMS	Lalwz	(847) 687-8198	Lar	Incoming
2010-12-25 (PST)	SMS	Stupid crashing computer	(847) 254-6108	El	Outgoing
2010-12-27 (PST)	MMS	Josh signing off for a while. It was fun	18472546108	El	Outgoing
2010-12-27 (PST)	MMS	<External Content>	18472546108	El	Outgoing
2010-12-27 (PST)	MMS	I'm out of here for a while. Dont try to reach me.	1 (847) 687-8198	Lar	Outgoing
2010-12-27 (PST)	MMS	<External Content>	1 (847) 687-8198	Lar	Outgoing
2010-12-27 (PST)	MMS	I'm out of here for a while. Dont try to reach me.	1 (847) 687-8198	Lar	Outgoing
2011-01-21 (PST)	SMS	Het just wanted to touch bases a. Did u find the car we talked about?	(408) 513-1851	Max Wayne	Outgoing
2011-01-21 (PST)	SMS	14085131851 Error Invalid Number. Please re-send using a valid 10 digit mobile numbe...	21611611	21611611	Incoming
2010-12-25 (PST)	SMS	Stupid crashing computer	(847) 254-6108	El	Outgoing

Attribute Value

ID:	284
Name:	sms.db
Path:	/mobile/Library/SMS
Size:	98304
Extension:	db
Content Type:	DB
Created:	2010-11-28 18:40
Modified:	2011-01-23 06:04
Accessed:	2011-01-23 06:04
Directory:	No
Visible:	Yes
Locked:	No
Fork Count:	1
MD5 Hash (Da...):	271E91EDB77F1F4F
Extents:	1
Physical Sector:	0
Logical Sector:	0
Logical Cluster:	-NAN(000)
FileNameOnDi...:	3D0D7E5FB2CE28881
OnDiskPathHa...:	3D0D7E5FB2CE28881
Metadata:Do...:	HomeDomain
Metadata:Path:	Library/SMS/sms.db
Metadata:Data...:	y
Metadata:Meda...:	22100

Full Message:

Het just wanted to touch bases a. Did u find the car we talked about?

View: Data Fork

(1 of 111) - /Josh Bennett's iPhone/mobile/Library/SMS/sms.db

Luca Mariani e Andrea Nardinocchi

MAC OS X FORENSICS

```
[...]
char *pointerextensions, defaultextensions[] = ".JPG.JPEG.GIF.PNG.RAW.PDF.MP3.WAV.MPG.MKV.AVI.DIVX.XVID.TIF.TIFF.TGA";
static char const * const defaultkeywords[] = { "PORN", "SEX", "CHILD", "NULL" };
int searchkey (const char *singleton) {
    int index = 0;
    while ((strcasecmp(defaultkeywords[index], "NULL")) != 0) {
        if (strcasestr(singleton, defaultkeywords[index]))
            return index;
        index++;
    }
    return -1;
}

int expand (const char *startpath, unsigned int deepsearch, float limit) {
    DIR *directory;
    struct dirent *informations;
    char *completepath, *extension;
    unsigned int completesize, elements = 0;
    int backupkeyword;
    float suspect = 0, percentage;
    if ((directory = opendir(startpath))) {
        while ((informations = readdir(directory))) {
            if ((strcmp(informations->d_name, ".") != 0) && (strcmp(informations->d_name, "..") != 0)) {
                if (informations->d_type == DT_DIR) {
                    completesize = strlen(startpath)+strlen(_dseparator)+strlen(informations->d_name);
                    if ((completepath = (char *) malloc (completesize+1))) {
                        /* generate the "complete" path name from the selected file so we can call it recursively */
                        snprintf(completepath, completesize, "%s%s%s", startpath, informations->d_name, _dseparator);
                        expand(completepath, (informations->d_name[0]=='.'), limit);
                        free(completepath);
                    } else return 1;
                } else if (deepsearch) { // searching for file's type
                    if (((extension = strchr(informations->d_name, '.')) && (strcasestr(pointerextensions, extension))) suspect++;
                    else if ((backupkeyword = searchkey(informations->d_name)) > 0) suspect++;
                    elements++;
                }
            }
        }
        if (deepsearch) {
            if (elements > 0) {
                percentage = ((float)(100 * suspect)/(float)elements);
                if (percentage > limit)
                    printf("\n[DIRECTORYSEARCH: notice]\n%s\n[total elements: %d] percentage %.1f of suspicious material\n\n",
startpath, elements, ((100.0*suspect)/elements));
            }
        }
        closedir(directory);
    } else return 1;
    return 0;
}
[...]
```

Luca Mariani e Andrea Nardinocchi

TARGET DISK MODE

T

Avviare la macchina in modalità **Target Disk**



Collegare la macchina attraverso un cavo Firewire (400/800 a seconda del modello) alla macchina dell'analista



Eseguire un **dump** completo dell'hard-disk attraverso software dedicati

Accessibilità completa ed incodizionata a tutti i dati presenti nella macchina

Luca Mariani e Andrea Nardinocchi



Keychain Access

Luca Mariani e Andrea Nardinocchi

MAC OS X FORENSICS



Click to lock the login keychain.

Keychains

- login
- System
- System Roots



tiredless

Kind: AirPort network password

Account: tiredless

Where: AirPort Network

Modified: Mar 23, 2011 11:37:46 PM

Name	Kind	Date Modified	Expires	Keychain
AIM: porcozizzo	application password	Mar 17, 2011 10:49:33 AM	--	login
@ aruba IMAP	Internet password	Mar 17, 2011 2:27:47 AM	--	login
com.apple.facetime: registration	application password	May 5, 2011 3:28:48 PM	--	login
Davide D'Arenzo	certificate	--	Nov 27, 2011 12:59:59 AM	login
Evernote				
FaceTime: nardinocchi@psychogames.net				
Google SketchUp				
Google SketchUp				
GoogleContactSyncService				
@ imap.gmail.com				
@ imap.psychogames.net				
@ imaps.aruba.it				
@ imaps.aruba.it				
@ imaps.psychogames.net				
nbugzilla.password				
radius.unipg.it				
Safari Forms AutoFill				
skype				
@ smtp.gmail.com				
@ smtp.psychogames.net				
@ smtps.aruba.it				
@ smtps.aruba.it				
@ smtps.psychogames.net				
tiredless	AirPort network pa...	Mar 23, 2011 11:37:46 PM	--	login
UTN-USERFirst-Client Authentication and Email	certificate	--	Jan 1, 2029 12:59:59 AM	login
@ www.psychogames.net	Internet password	Mar 17, 2011 5:10:28 PM	--	login
@ www.psychogames.net	Internet password	Mar 17, 2011 5:10:29 PM	--	login

tiredless

Attributes Access Control

Name: tiredless

Kind: AirPort network password

Account: tiredless

Where: AirPort Network

Comments:

☐ Show password:

Save Changes

Luca Mariani e Andrea Nardinocchi

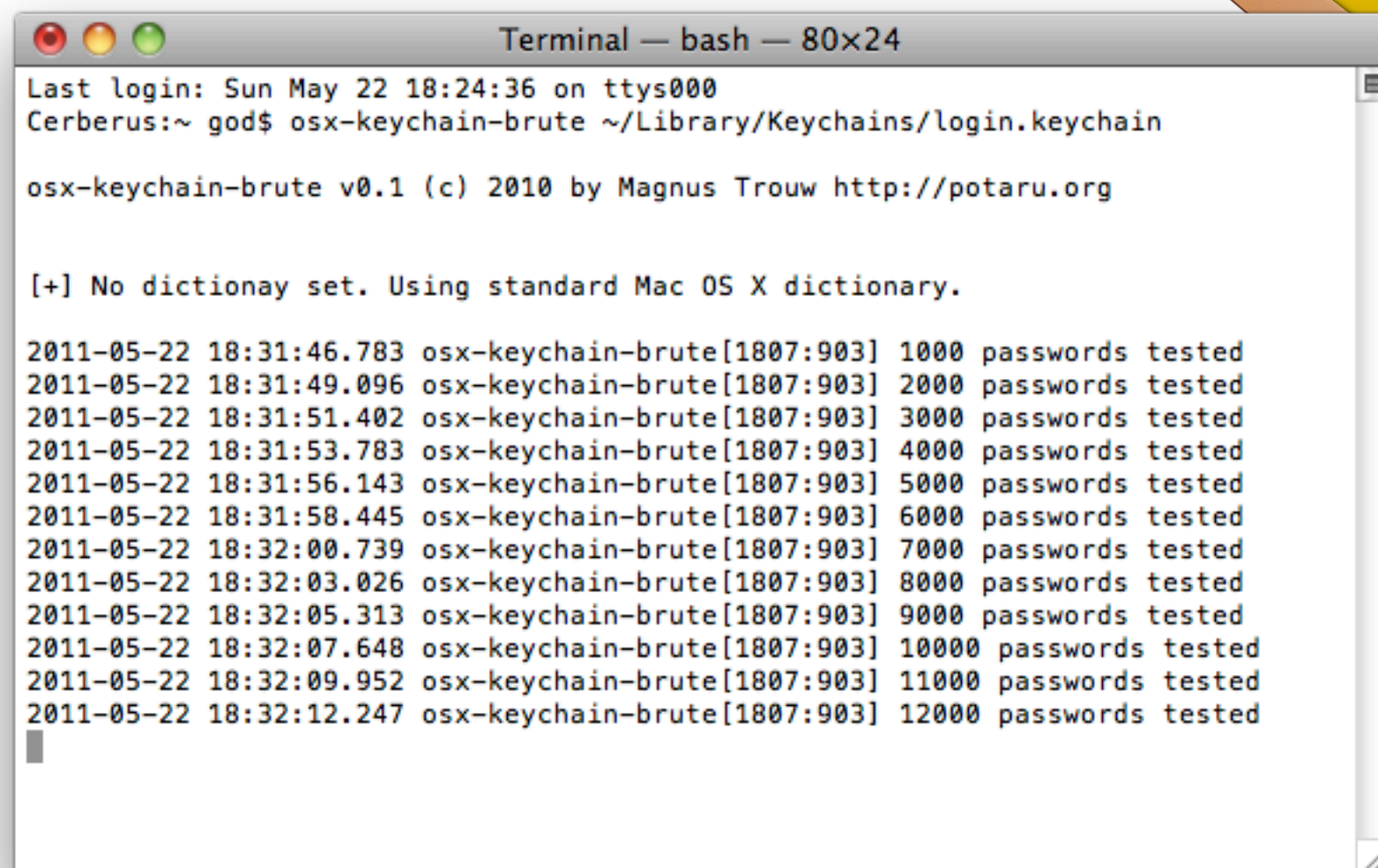
BRUTEFORCE VS KEYCHAIN ACCESS

TOOL: osx-keychain-brute

Dizionario personalizzabile

Estremamente **Rapido** (controllo di 60.000 termini in un minuto e trenta secondi circa)

Utilizzo immediato



```
Terminal — bash — 80x24
Last login: Sun May 22 18:24:36 on ttys000
Cerberus:~ god$ osx-keychain-brute ~/Library/Keychains/login.keychain

osx-keychain-brute v0.1 (c) 2010 by Magnus Trow http://potaru.org

[+] No dictionary set. Using standard Mac OS X dictionary.

2011-05-22 18:31:46.783 osx-keychain-brute[1807:903] 1000 passwords tested
2011-05-22 18:31:49.096 osx-keychain-brute[1807:903] 2000 passwords tested
2011-05-22 18:31:51.402 osx-keychain-brute[1807:903] 3000 passwords tested
2011-05-22 18:31:53.783 osx-keychain-brute[1807:903] 4000 passwords tested
2011-05-22 18:31:56.143 osx-keychain-brute[1807:903] 5000 passwords tested
2011-05-22 18:31:58.445 osx-keychain-brute[1807:903] 6000 passwords tested
2011-05-22 18:32:00.739 osx-keychain-brute[1807:903] 7000 passwords tested
2011-05-22 18:32:03.026 osx-keychain-brute[1807:903] 8000 passwords tested
2011-05-22 18:32:05.313 osx-keychain-brute[1807:903] 9000 passwords tested
2011-05-22 18:32:07.648 osx-keychain-brute[1807:903] 10000 passwords tested
2011-05-22 18:32:09.952 osx-keychain-brute[1807:903] 11000 passwords tested
2011-05-22 18:32:12.247 osx-keychain-brute[1807:903] 12000 passwords tested
```

Luca Mariani e Andrea Nardinocchi



FileVault

Luca Mariani e Andrea Nardinocchi



Software per l'analisi

- Creazione di copie forensi del disco in esame;
- Analisi;
- Blocco della scrittura.





BlackBag

Fornisce soluzioni per l'analisi forense di sistemi Mac e dati eDiscovery.

I maggiori prodotti sono:

- MacQuisition, per la creazione delle immagini;
- BlackLight, per l'analisi dei supporti;
- SoftBlock, per bloccare la scrittura sui supporti.



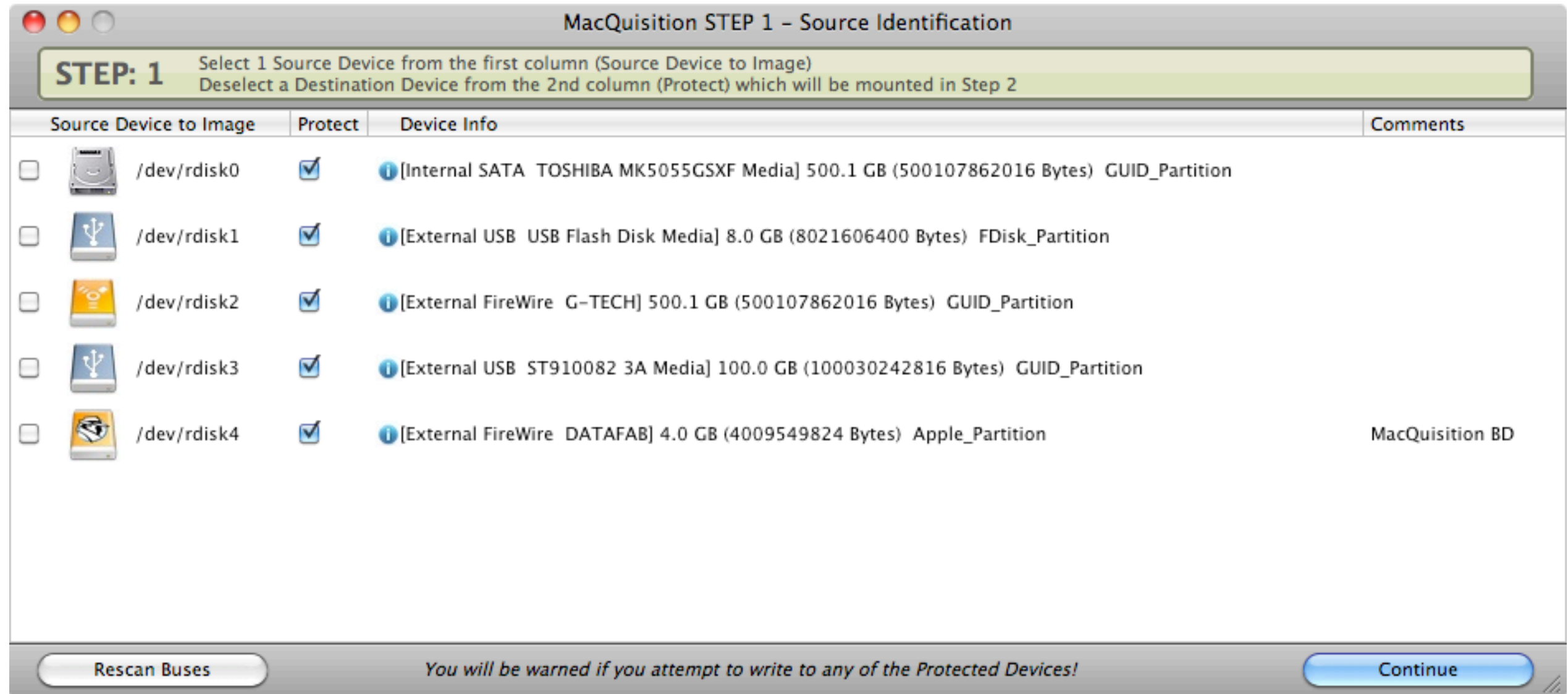
Si basa direttamente sul sistema operativo OS X, utilizzandolo per creare l'immagine. Facile da utilizzare sia sul campo che in laboratorio, in cinque semplici passi crea l'immagine del supporto desiderata.



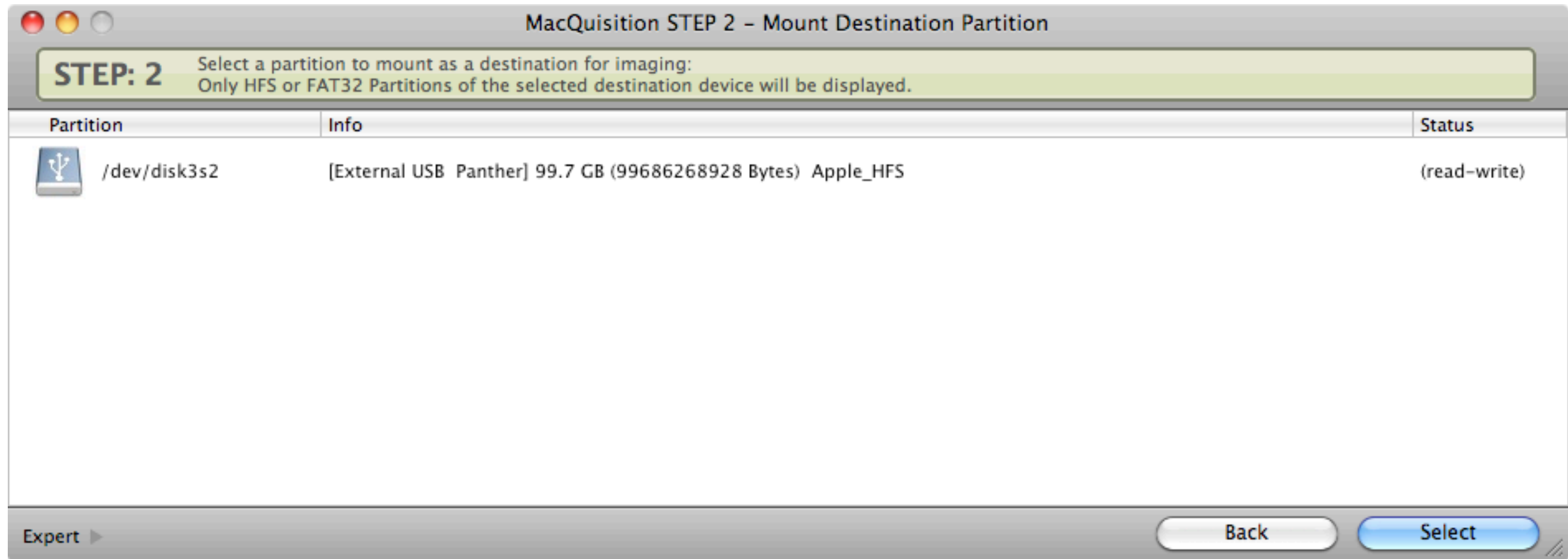
Costo: 599.00\$

MacQuisition

Luca Mariani e Andrea Nardinocchi



Passo I: Identificazione del supporto.



Passo 2: Selezione della destinazione della partizione.

MacQuisition STEP 3 - Case Information

STEP: 3 Enter the specific case details such as current time zone and case name.
Set the Case ID, Exhibit ID, and Image Name before you continue.

System Time: 2011-01-18 02:46:31 (UTC) Case ID: CASE_0001

Time Zone: Pacific Standard Time ☐ Daylight Savings Exhibit ID: EXHIBIT_0001

Local Time: 2011-01-17 18:46:20 Image Name: IMAGE_0001

Case Name: CASE123

Location: San Jose

Folder Name: CASE123_2011-01-17_184620

Additional Information

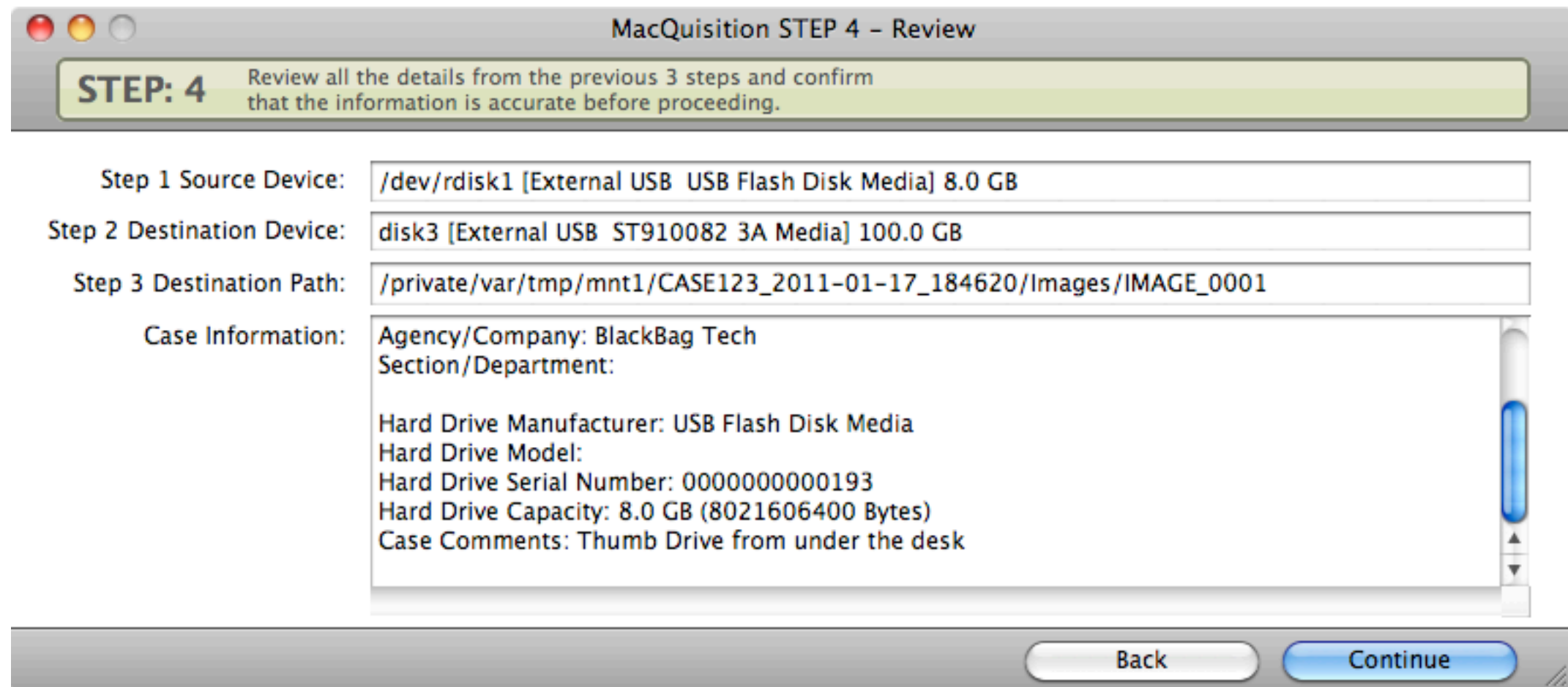
Advanced Options

☒ Segmented Image ☒ .dmg Extensions

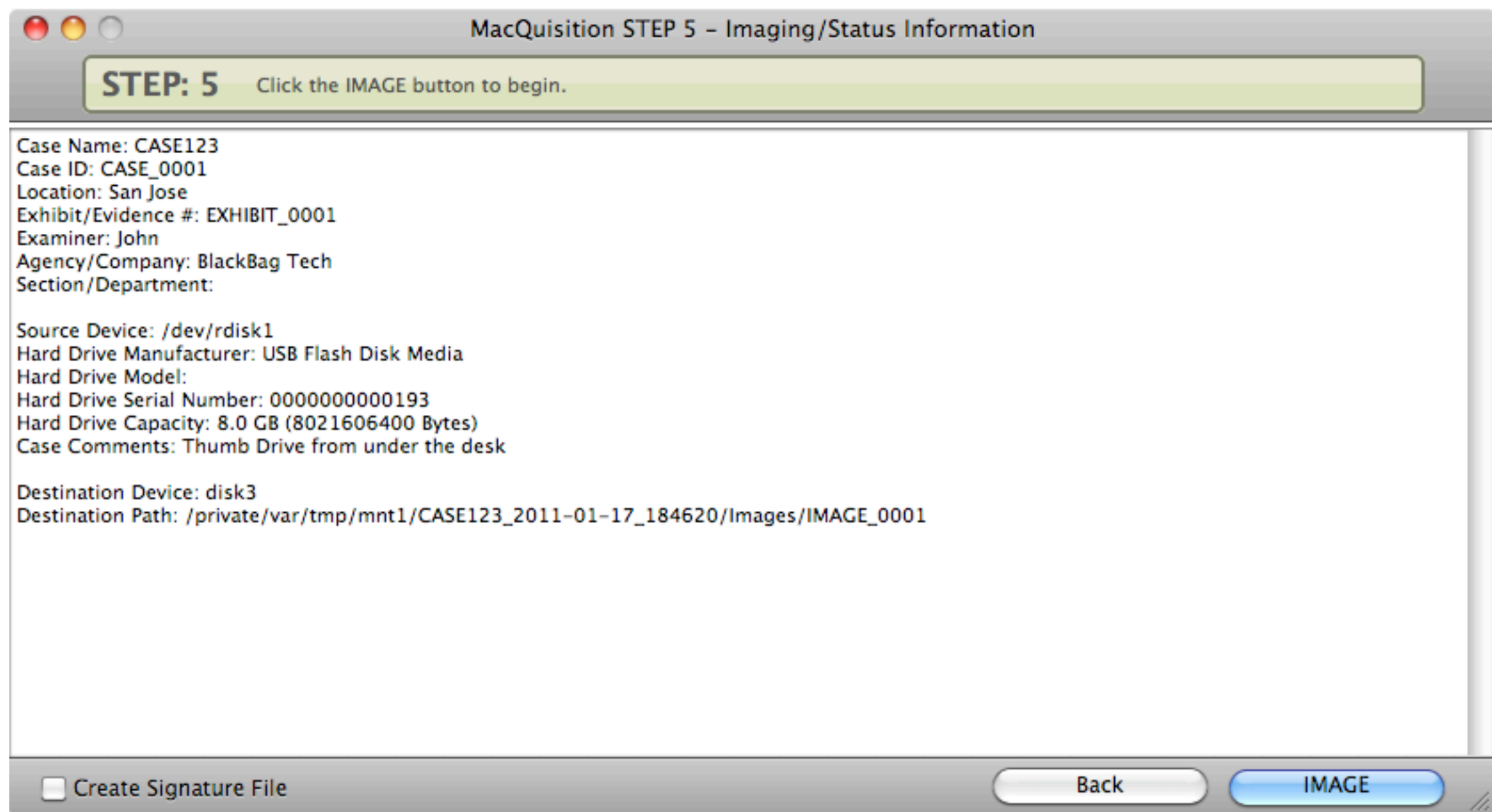
2 GB ☐ .001 Extensions

Back Continue

Passo 3: Inserimento delle informazioni.



Passo 4: Controllo delle informazioni fornite.



Passo 5: Inizio del processo di creazione dell'immagine.

MacQuisition

Luca Mariani e Andrea Nardinocchi

Piattaforma intuitiva che permette di cercare, trovare, analizzare e riportare dati da Mac e iOS.

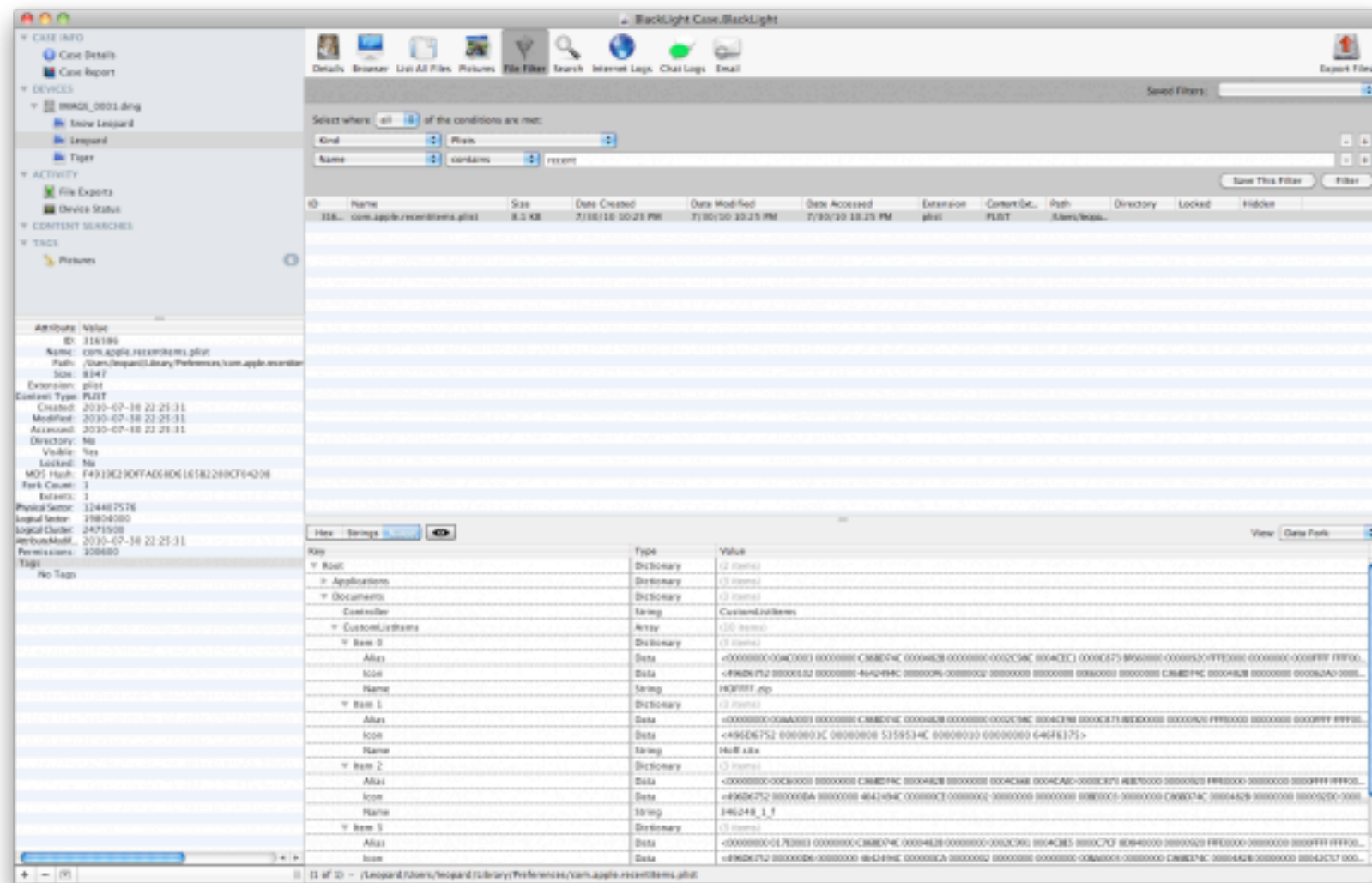
- iOS : backup completo, hash dei file, analisi dei file e delle firme, recupero file eliminati (SQLite Recovery Feature).
- Mac: identifica dei file a seconda delle estensioni, separando file di sistema conosciuti da quelli sospetti; analizza e identifica le immagini, fornendo numerose opzioni di ordinamento; analisi sulla cronologia dei browser e delle chat.



Costo: 2,499.00\$

BlackLight

Luca Mariani e Andrea Nardinocchi



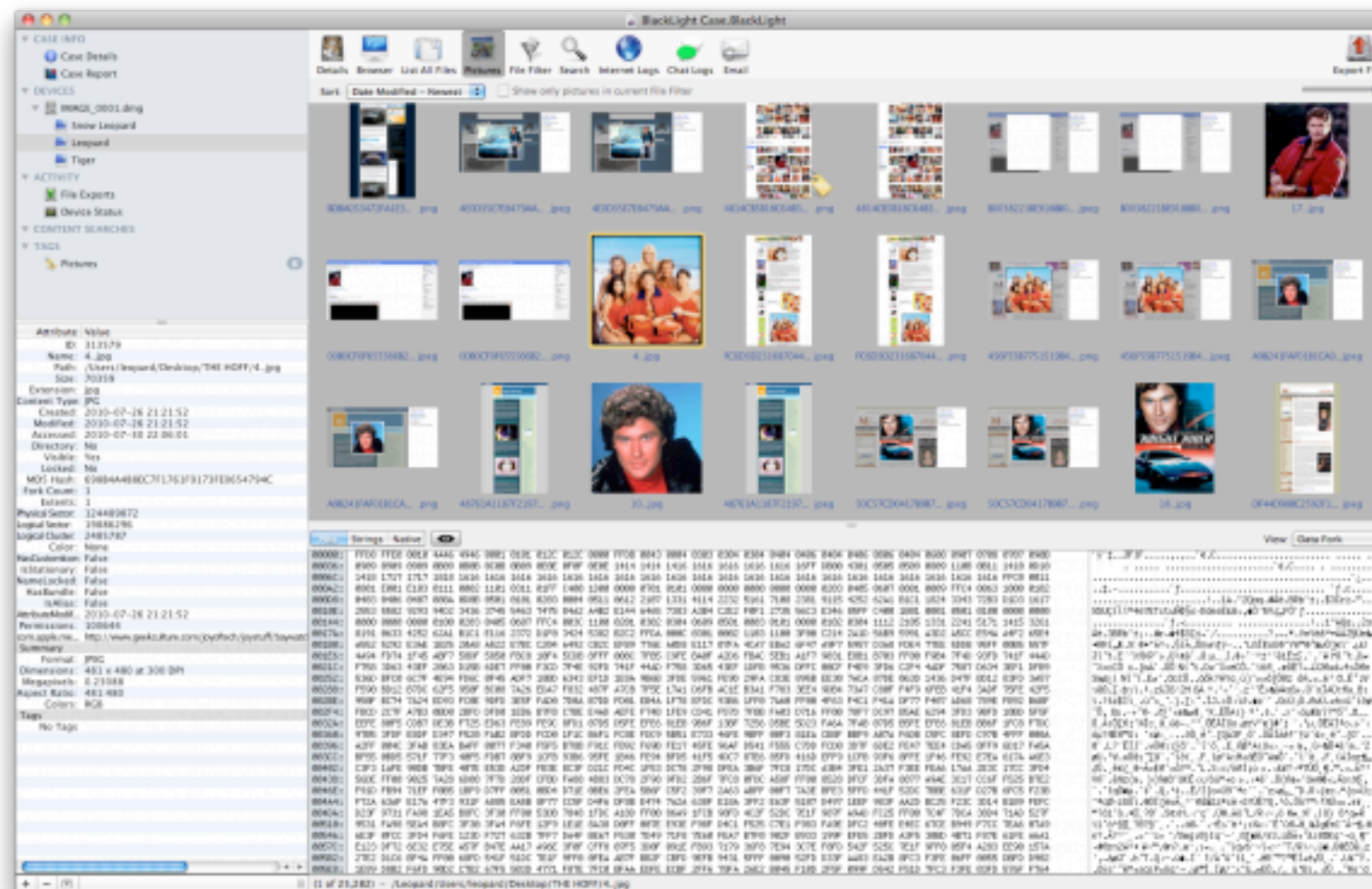
Per ogni file, viene fornita una lista di dati tra i quali la cartella in cui è contenuto, la data dell'ultima modifica e la data dell'ultimo accesso.

Riconoscimento dei file di sistema dalla versione 10.0.0 alla versione 10.6.7.

BlackLight

Luca Mariani e Andrea Nardinocchi

Funzione di riconoscimento delle immagini.
Numerose opzioni di ordinamento, tra le quali anche
l'analisi in base al colore della pelle.



BlackLight

Luca Mariani e Andrea Nardinocchi

Prodotto ideato per analizzare e avere una preview di uno o più eventuali supporti probatori.
Possibilità di dare un primo sguardo a possibili prove, identificando i dispositivi al momento della connessione e, a seconda delle preferenze, montandoli sia in sola lettura, sia in lettura-scrittura, senza la necessità di utilizzare programmi di protezione.

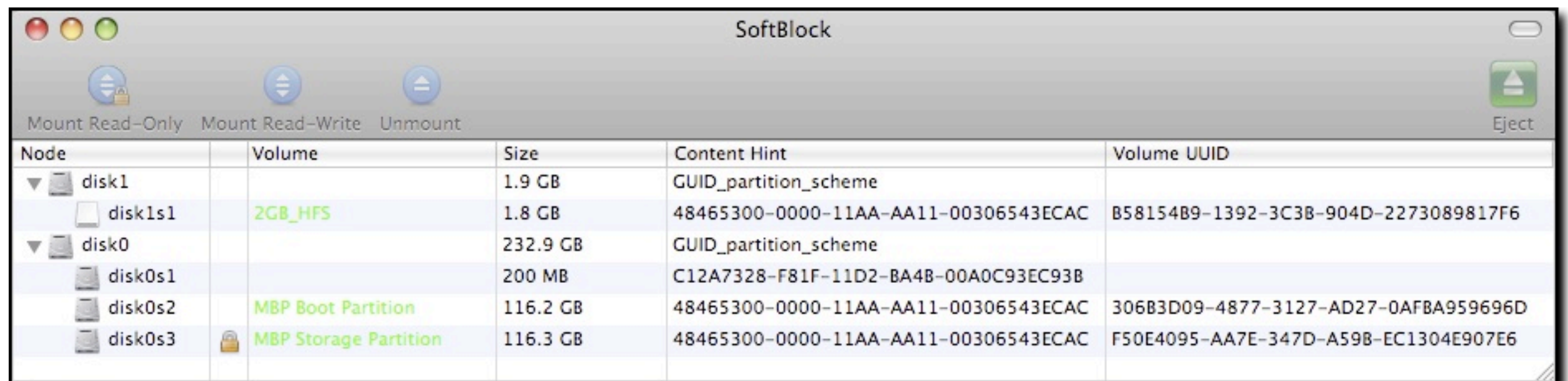


Costo: 239.00\$

SoftBlock

Luca Mariani e Andrea Nardinocchi

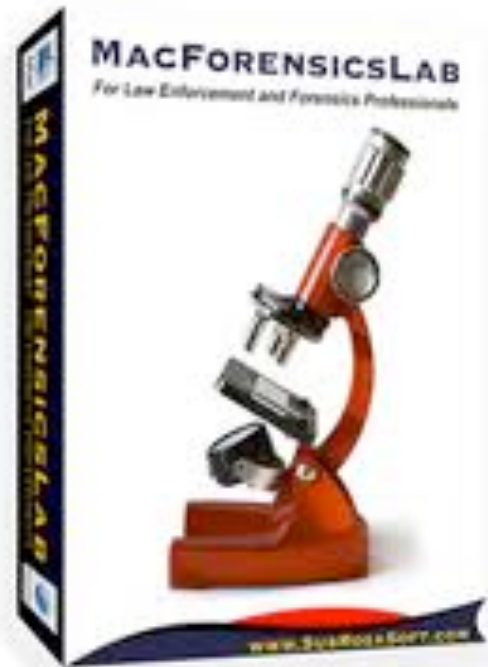
MAC OS X FORENSICS



SoftBlock

Luca Mariani e Andrea Nardinocchi

MacForensicsLab

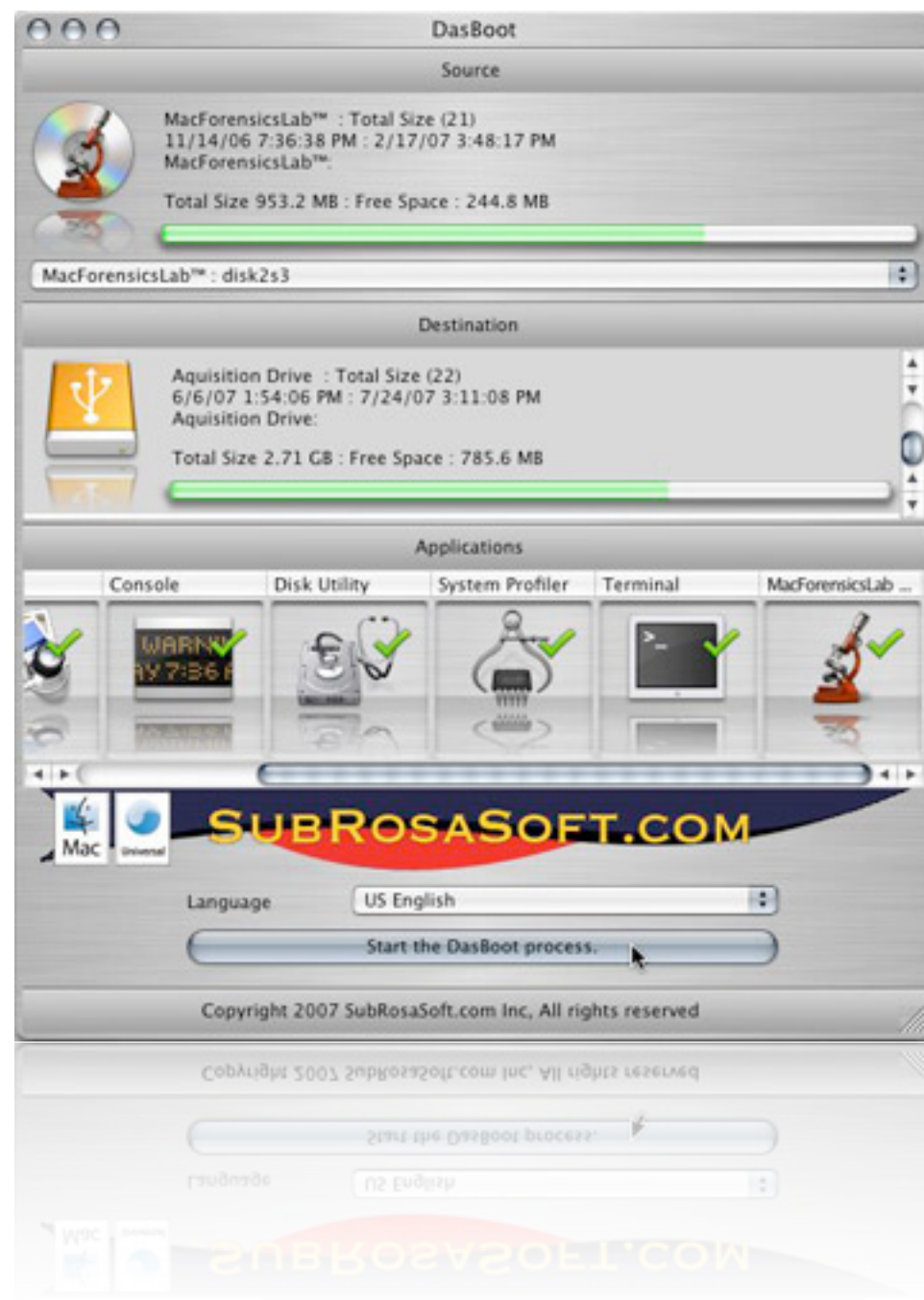


Costo: 1,495.00\$

Funzionamento su
ogni tipo di piattaforma.
Veloce, alta tolleranza d'errore e
possibilità di verificare le acquisizioni.

MacForensicsLab

Luca Mariani e Andrea Nardinocchi



Consente la creazione di una replica esatta del supporto originario, massimizzando anche il recupero dei dati corrotti. Immagini create mediante un hashing integrato. Consente la duplicazione delle immagini e dei file di hash associati.

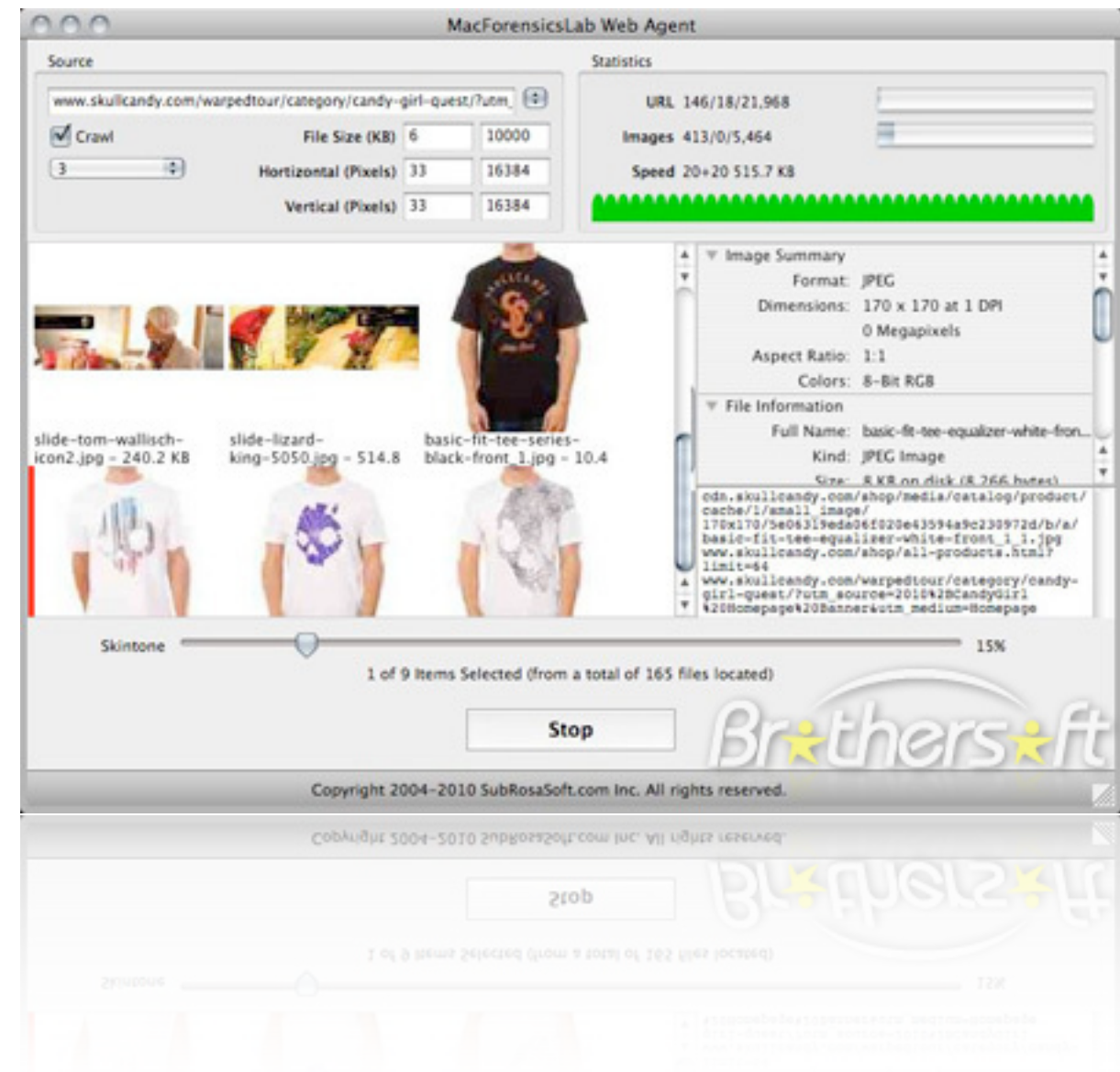
MacForensicsLab

Luca Mariani e Andrea Nardinocchi

Creazione di anteprime di immagini grafiche, filtrate automaticamente in base ai toni della pelle, al tipo di immagine e alla dimensione del file.

Funzione di ricerca con parole chiave, catalogazione in base a differenti lingue, ricerca di numeri di codice fiscale e carte di credito.

MacForensicsLab



Luca Mariani e Andrea Nardinocchi

The Sleuth Kit



Costo: Freeware

Progetto Open Source per fornire tools digitali per l'investigazione forense.

Raccolta di linee comando utilizzabili su Windows e sistemi Unix.

- The Sleuth Kit
- Autopsy

Luca Mariani e Andrea Nardinocchi

Utilizzabile in due modi differenti:
implementazione con altri software di ricerca;
utilizzo diretto delle linee comando.

Esempio: ricerca di una stringa

```
# blkls images/wd0e.dd > output/wd0e.blkls
# strings -t d output/wd0e.blkls > output/wd0e.blkls.str
# grep abcdefg output/wd0e.blkls.str | less
  10389739: abcdefg
# fsstat openbsd images/wd0e.dd
<...>
CONTENT-DATA INFORMATION
-----
Fragment Range: 0 - 266079
Block Size: 8192
Fragment Size: 1024
# dd if=images/wd0e.dd bs=1024 skip=10146 count=1 | less
# blkcalc -u 10146 images/wd0e.dd
  59382
# blkcat images/wd0e.dd 59382 | less
```

Estrazione unità disco non allocata
Estrazione di tutte le stringhe
Ricerca della stringa

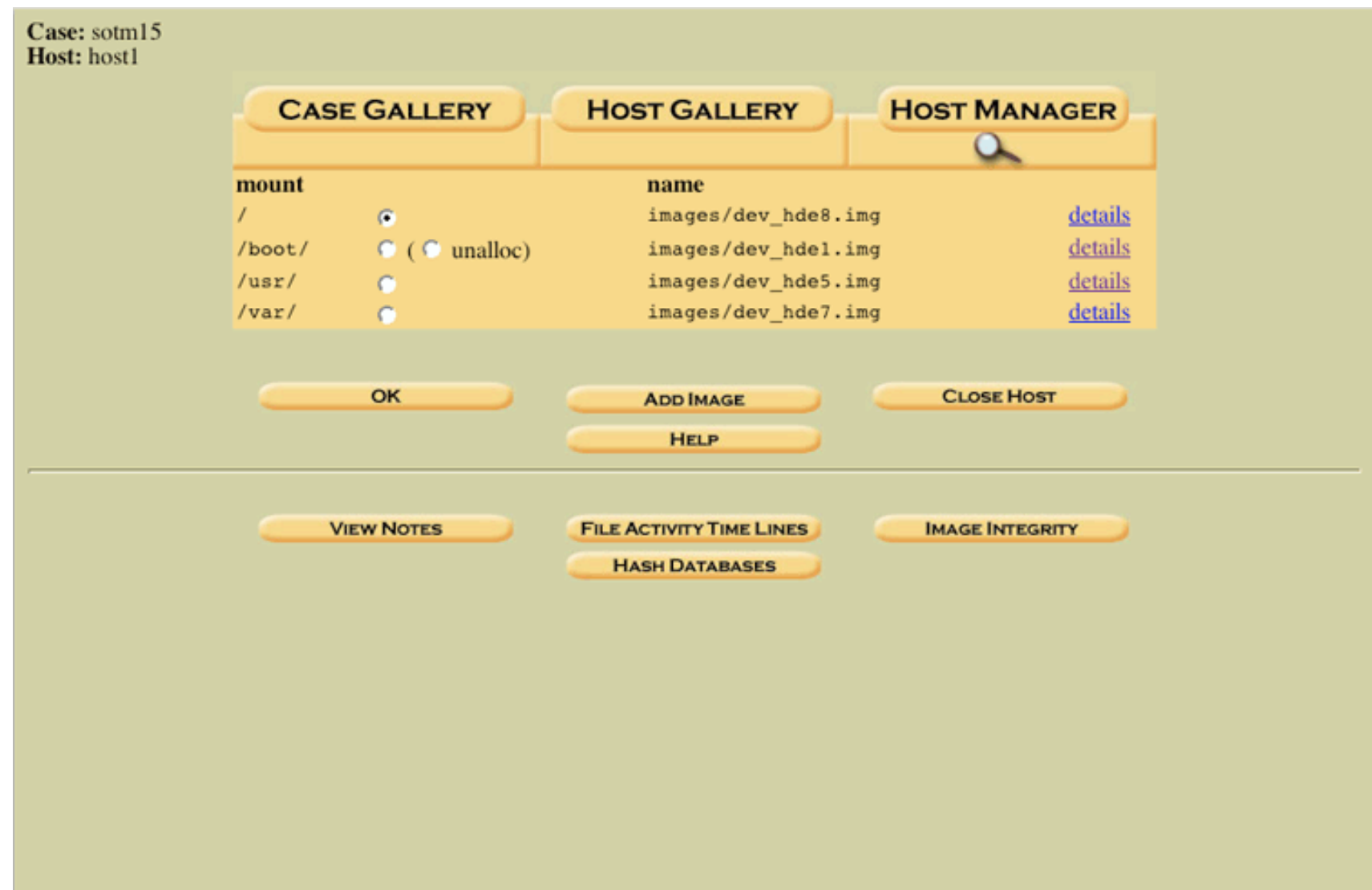
Determinazione del frammento in cui è
posizionata la stringa

Esame dell'intero frammento dall'immagine
Ricerca dell'allocazione dell'immagine
Visualizzare il contenuto del frammento
trovato.

Interfaccia grafica del kit, che mostra dettagli riguardo a file rimossi e struttura del file system.

Dead Analysis: Un sistema di analisi dedicato viene utilizzato per esaminare dati da un sistema sospetto.

Live Analysis: Il sistema sospetto viene analizzato mentre è in funzione.



Autopsy

Luca Mariani e Andrea Nardinocchi

Costo: Freeware

dcfldd

Tool Unix basato sul comando GNU dd.

Supporta l'hashing dei dati quando viene creata l'immagine del disco, permettendo la verifica del fatto che l'immagine non sia stata modificata dalla sua acquisizione.

E' in grado di verificare se sono state eliminate immagini, proteggere l'integrità dei dati, dare più risultati contemporaneamente categorizzandoli in maniera personalizzabile.

dcfldd

Luca Mariani e Andrea Nardinocchi

Esempio:

```
dcfldd if=/dev/sourcedirve hash=md5,sha256 hashwindow=10G md5log=md5.txt sha256log=sha256.txt \  
hashconv=after bs=512 conv=noerror,sync split=10G splitformat=aa of=driveimage.dd
```

Legge 10 gigabyte dal supporto originale e li scrive nel file chiamato driveimage.dd.aa. Calcola l'hash MD5 dei 10 Gb, leggendo poi i dieci Gb successivi e denominando il file generato driveimage.dd.ab.

dcfldd

Luca Mariani e Andrea Nardinocchi

Grazie per l'attenzione

Luca Mariani e Andrea Nardinocchi