Hacker Highschool
SECURITY AWARENESS FOR TEENS

LEZIONE 8
DIGITAL FORENSICS

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

“License for Use” Information

The following lessons and workbooks are open and publicly available under the following terms and conditions of ISECOM:

All works in the Hacker Highschool project are provided for non-commercial use with elementary school students, junior high school students, and high school students whether in a public institution, private institution, or a part of home-schooling. These materials may not be reproduced for sale in any form. The provision of any class, course, training, or camp with these materials for which a fee is charged is expressly forbidden without a license including college classes, university classes, trade-school classes, summer or computer camps, and similar. To purchase a license, visit the LICENSE section of the Hacker Highschool web page at www.hackerhighschool.org/license.

The HHS Project is a learning tool and as with any learning tool, the instruction is the influence of the instructor and not the tool. ISECOM cannot accept responsibility for how any information herein is applied or abused.

The HHS Project is an open community effort and if you find value in this project, we do ask you support us through the purchase of a license, a donation, or sponsorship.

All works copyright ISECOM, 2004.

Informazioni sulla licenza d’uso

Le seguenti lezioni ed il materiale per gli esercizi (workbook) sono materiale di tipo "open" e pubblicamente disponibili, secondo i seguenti termini e condizioni di ISECOM:

Tutto il materiale inerente il progetto Hacker Highschool è fornito esclusivamente per utilizzo formativo di tipo “non-commerciale” verso gli studenti delle scuole elementari, medie e superiori ed in contesti quali istituzioni pubbliche, private e/o facenti parte di attività del tipo “doposcuola”.

Il materiale non può essere riprodotto ai fini di vendita, sotto nessuna forma ed in nessun modo.

L’erogazione di qualunque tipologia di classe, corso, formazione (anche remota) o stage tramite questo materiale a fronte del corrispondimento di tariffe o denaro è espressamente proibito, se sprovvisti di regolare licenza, ivi incluse classi di studenti appartenenti a college, università, trade-schools, campi estivi, invernali o informatici e similari.

Per comprendere le nostre condizioni di utilizzo ed acquistare una licenza per utilizzi di tipo commerciale, vi invitiamo a visitare la sezione LICENSE del sito web Hacker Highschool all’indirizzo http://www.hackerhighschool.org/license.

Il Progetto HHS è uno strumento per apprendere e, come ogni strumento di questo tipo, la chiave formativa consiste nella capacità e nell'influenza dell'istruttore, e non nello strumento formativo. ISECOM non può accettare e/o farsi carico di responsabilità per il modo in cui le informazioni qui contenute possono essere utilizzate, applicate o abusate.

Il Progetto HHS rappresenta uno sforzo di una comunità aperta: se ritenete il nostro lavoro valido ed utile, vi chiediamo di supportarci attraverso l'acquisto di una licenza, una donazione o una sponsorizzazione al progetto.

Tutto il materiale e' sotto copyright ISECOM, 2004

Indice

Contributors

Simon Biles, Computer Security Online Ltd.

Pete Herzog, ISECOM

Chuck Truett, ISECOM

Marta Barceló, ISECOM

Kim Truett, ISECOM

Per la versione in lingua italiana:

Raoul Chiesa, ISECOM

Doriano Azzena, centro CSAS del progetto Dschola IPSIA Castigliano - Asti

Sophia Danesino, centro CSAS del progetto Dschola ITIS Peano – Torino

Nadia Carpi, centro CSAS del progetto Dschola ITIS Peano – Torino

Fabrizio Sensibile, OPST&OPSA Trainer, @ Mediaservice.net Srl, Torino - ISECOM Authorized Training Partner

Claudio Prono, @ Mediaservice.net Srl, Torino – ISECOM Authorized Training Partner

8.0 Introduzione

Le attività forensi identificano l'applicazione di tecniche metodiche di ricerca per ricostruire una serie d'eventi. La maggior parte delle persone ora ha familiarità con il concetto di forense dalla TV e dalle pellicole cinematografiche, in cui "l'investigazione sulla scena del crimine" è una delle situazioni più ricorrenti e popolari. La scienza forense sì é occupata a lungo - ed é ancora fortemente collegata con la Patologia Legale – di scoprire com'é morta la gente. La prima descrizione scritta di forense risale al 1248 anno in cui fu pubblicato un libro cinese denominato Hsi DuanYu (spazzare via i torti). Questo libro descrive come dire se qualcuno è annegato o è stato strangolato.

Il digitale forense è un po' meno "sporco" e un po' meno conosciuto. Esso è l'arte di ricreare che cosa è accaduto in un dispositivo digitale. Nel passato il digitale forense era limitato soltanto ai calcolatori; ora comprende tutti i dispositivi digitali tra cui i telefoni mobili, le macchine fotografiche digitali e perfino i dispositivi GPS. È stato usato per smascherare assassini, rapitori di bambini, truffatori, boss mafiosi e molta altra gente certamente poco raccomandabile.

In questa lezione, tratteremo due aspetti del digitale forense che si riferiscono ai computer, non tratteremo la telefonia mobile.

1. Cosa ha fatto un utente sul proprio computer.

Ovvero ...

- ... il recupero dei file cancellati.
- ... descrizione elementare.
- ... ricerca di alcuni tipi di file.
- ... ricerca di alcune frasi.
- ... esame di aree interessanti del computer.

2. Cosa ha fatto un utente remoto sul computer di qualcun altro.

Ovvero ...

- ... leggere I file di log.
- ... ricostruire azioni.
- ... tracciare la sorgente.

Questa lezione tratta degli strumenti disponibili sotto Linux. Ci sono strumenti che sono disponibili sotto Windows, come pure software e hardware dedicato per svolgere attività forensi, ma la possibilità offerta da Linux di riconoscere altri sistemi e file system, ne fanno l'ambiente ideale per la maggior parte delle indagini forensi.

8.1 Principi forensi

8.1.0 Introduzione

Ci sono un certo numero di principi di base che sono necessari indipendentemente dal fatto che intendiate esaminare un computer o un altro corpo di reato. Questa sezione è un sommario sintetico di questi principi.

8.1.1 Evitate la contaminazione

Sulla TV vedete gli ispettori legali, vestiti di bianco con i guanti, maneggiare tutte le prove con le pinzette e metterle in sacchetti di plastica sigillati. Tutto ciò al fine di prevenire la contaminazione delle prove.

Questo è la fase in cui le prove possono essere alterate, per esempio, l'aggiunta delle impronte digitali sul manico di un coltello da parte di qualcuno che lo impugna inavvertitamente (pensate a "Il fuggitivo" se lo avete visto... ricordate a quali difficoltà va incontro!).

8.1.2 Agite con metodo

Nell'ipotesi in cui sarete chiamati a presentarvi davanti al tribunale, preparatevi a giustificare tutte le azioni che avete intrapreso. Comportatevi in modo scientifico e metodico, annotate tutto ciò che state facendo e come lo fate, riuscirete più facilmente a fornire le giustificazioni richieste e a permettere ad altri di ripetere le vostre azioni e verificare che non abbiate commesso errori che possono invalidare il valore della vostra prova.

8.1.3 Chain of Evidence

Dovete mantenere un documento denominato "Chain of evidence" (la catena delle prove) su cui tenere traccia di tutte le operazioni e movimentazioni delle possibili fonti di prova. Ciò significa che ad un qualunque punto del tempo intercorrente tra la presa in carico delle prove e la presentazione finale in tribunale, dovete poter documentare chi ha avuto accesso alle prove e dove è stato. L'esistenza della "chain of evidence" elimina la possibilità dell'alterazione o falsificazione delle prove da parte di qualcuno.

8.1.4 Conclusioni

Tenete a mente queste cose ed anche se non presenterete il vostro lavoro in tribunale, potrete migliorare le vostre abilità come ispettore legale.

8.2 Pratiche forensi Stand-alone

8.2.0 Introduzione

Questa sezione riguarda l'analisi forense di un computer singolo in seguito indicata come "forense stand-alone". La pratica forense stand-alone è probabilmente la parte più comune dell'attività forense rivolta ai computer, il suo obiettivo principale è quello di scoprire che cosa è stato fatto per mezzo di un particolare computer. L'ispettore forense potrebbe cercare la prova della frode, quali i fogli elettronici finanziari, la prova della comunicazione con qualche altra persona, E-mail in un indirizzario, o prove di natura particolare, quali le immagini pornografiche.

8.2.1 Hard Disk e fondamenti sui dispositivi di memorizzazione

Ci sono parecchi componenti che compongono un calcolatore medio. Ci sono il processore, la memoria, la scheda grafica, i dispositivi CD e altro ancora. Uno dei componenti cruciali è il disco rigido (hard disk); esso è il dispositivo in cui risiede la maggior parte delle informazioni che il calcolatore richiede per funzionare. Il sistema operativo (OS) quale Windows o Linux risiede sul disco rigido con le applicazioni dell'utente quali i programmi di trattamento di testi ed i giochi. Il disco rigido è anche il luogo dov'è memorizzata la maggior parte dei dati, deliberatamente, per mezzo di una operazione "salva file" o incidentalmente con l'uso di file temporanei e della cache (memoria deputata a mantenere programmi e dati per permettere un accesso rapido ad essi senza la necessità di richiamarli). Ciò permette ad un ispettore forense di ricostruire le azioni che l'utente ha effettuato su un calcolatore, quali file ha consultato e molto, molto di più.

Ci sono parecchi livelli a cui potete esaminare un hard disk. Per gli scopi di questa esercitazione, prendiamo in considerazione soltanto il livello del file system. Vale la pena di notare in ogni caso, che i professionisti sono in grado di esaminare un livello maggiore di dettaglio per determinare il contenuto di un hard disk anche se è stato soprascritto molte volte.

Il file system è l'implementazione del calcolatore di un casellario. Esso contiene i cassetti (partizioni), le cartelle (directory) e diversi fogli di carta (file). File e directory possono essere nascosti, anche se questa è soltanto una cosa superficiale e può essere facilmente aggirata.

Eseguire le seguenti esercitazioni dovrebbe darvi una comprensione migliore dei principi fondamentali dei dischi di memorizzazione.

Esercizi

Per ciascuno dei seguenti termini cercate informazioni ed imparate come funzionano i dispositivi di memorizzazione. Il vostro primo passo verso il digitale forense consiste normalmente nel capire come funzionano le apparecchiature.

1. Magnetic/Hard/Physical Disk: il dispositivo su cui il vostro computer memorizza i file. Spiegate come il magnetismo è utilizzato su un hard disk.

2. Tracks (tracce): Cosa si intende per "tracce" in un hard disk?

3. Sectors (settori): rappresentano uno spazio fisso in cui trovano posto i dati. Spiegate come.

4. Cluster/Allocation unit: Spiegate perchè quando un file è scritto su un hard disk può darsi che gli sia assegnato più spazio di quanto bisogna. Cosa succede a questo spazio vuoto? Cercate "file slack" dovrebbe aiutarvi.

5. Free/"Unallocated" Space: E' ciò che rimane dopo aver cancellato I file. I file sono realmente spariti? Spiegate come un file è cancellato sul computer. Cercare strumenti per la cancellazione sicura (secure delete) può aiutarvi. Supponendo che sappiate come cancellare in modo sicuro un file è bene conoscere perché sono necessari tali strumenti.

6. Hash, anche noto come MD5 hash: Spiegate che cosa è e per cosa è utiizzato.

7. BIOS: Significa "Basic Input/Output System". Cosa è e dove si trova nel PC?

8.Boot Sector: Funziona con le tabelle di partizione per aiutare il vostro PC a trovare il sistema operativo da utilizzare. Ci sono molti strumenti per lavorare con le partizioni, quello standard è denominato fdisk. Sapere come lavorano questi strumenti è il vostro primo passo per capire le partizioni e il settore di boot.

9. Cyclical Redundancy Check (CRC): Quando ottenete il messaggio "read error" dal vostro hard disk, significa che I dati non hanno superato il test CRC. Cercate che cosa è il CRC e che cosa fa.

10. File Signature: Spesso all'inizio di un file si trova una piccola firma composta di 6-byte che identifica di che tipo di file si tratta. Aprire un file con un editore di testo (text editor) è il modo più semplice per vedere la firma. Aprite 3 file dei seguenti tipi con un editore di testo: .jpg, .gif, .exe, .mp3. Quale è la prima parola all'inizio di ciascun file?

11. RAM (Random-Access Memory): Anche nota come "memoria" è il dispositivo in cui le informazioni sono scritte (write) e lette (read) in modo temporaneo, ovvero non permanente. Le operazioni di scrittura e di lettura avvengono molto più velocemente che su un hard disk. La mancata alimentazione significa la perdita delle informazioni. Spiegate come lavorano le RAM. Sapendo che il vostro PC può avere una quantità di memoria che varia da 64 a 512 Mb di RAM, cercate informazioni su un computer che supporta una maggiore quantità di RAM.

Attualmente, il più grande RAM disk (un hard disk super veloce emulato in RAM) é di 2.5 Tb (Terabyte). Quante volte maggiore del disco rigido del vostro PC?

8.2.2 Cifrare, Decifrare e formati dei file

Una parte dei file che incontrerete non sarà immediatamente leggibile. Molti programmi hanno i formati proprietari dei file, mentre altri usano i formati standard - per esempio gli standard per le immagini - GIF, JPEG, ecc. Linux fornisce un'eccellente programma di utilità per aiutarti a determinare che cosa è un dato file. Esso é denominato **file.**

Command Line Switch	Effect
-k	Don't stop at the first match, keep going.
-L	Follow symbolic links
-z	Attempt to look inside compressed files.

Segue un esempio dell'uso del commando file:

```
[simon@frodo file_example]$ ls
arp.c nwrap.pl
isestorm_DivX.avi oprp_may11_2004.txt
krb5-1.3.3 VisioEval.exe
krb5-1.3.3.tar Windows2003.vmx
krb5-1.3.3.tar.gz.asc

[simon@frodo file_example]$ file *
arp.c: ASCII C program text
isestorm_DivX.avi: RIFF (little-endian) data, AVI
krb5-1.3.3: directory
krb5-1.3.3.tar: POSIX tar archive
krb5-1.3.3.tar.gz.asc: PGP armored data
nwrap.pl: Paul Falstad's zsh script text executable
oprp_may11_2004.txt: ASCII English text, with very long lines, with CRLF
line terminators
VisioEval.exe: MS-DOS executable (EXE), OS/2 or MS Windows
Windows2003.vmx: a /usr/bin/vmware script text executable
[simon@frodo file_example]$
```

Da qui potete cominciare a fare qualche tentativo per leggere un certo tipo di file. In linux ci sono un certo numero di utilità per la conversione dei file e per la visualizzazione dei vari formati dei file. Per arrivare al punto in cui potete realmente lavorare con i dati a volte, sono necessari più passi.

Occasionalmente incontrerete file che sono stati cifrati o protetti da password. La complicazione che si presenta varia, dalla cifratura che è facilmente decifrabile a quella in grado di procurare il mal di testa agli esperti. Ci sono ancora un certo numero di strumenti disponibili su Internet che potete usare per provare a decifrare i file o le password. Vale la pena esaminare l'area che circonda il PC (p.es. la scrivania). Le persone non ricordano facilmente le password e a volte le annotano da qualche parte vicino al PC. Le scelte più comuni per le parole d'accesso inoltre coinvolgono: animali domestici, parenti, date (matrimonio, data di nascita), numeri di telefono, registri dell'automobile ed altre combinazioni semplici (123456, abcdef, ecc. qwerty). Gli utenti inoltre non gradiscono usare più di una o due parole d'accesso per tutto, se riuscite a decifrare la password per un file o applicazione, provate la medesima anche con gli altri, potrebbe funzionare. È' molto probabile che funzioni.

Esercizi

In questi esercizi, impareremo i fondamenti del password cracking (decifrare le parole di accesso). Ricordate che è legale decifrare le vostre parole d'accesso se le avete dimenticate; in alcuni paesi non è legale esaminare com'è cifrato qualcos'altro, per proteggere altro materiale dall'essere decifrato (cracked).

I film su DVD sono cifrati per impedire di essere estratti dal DVD ed essere venduti. Mentre questo è un uso eccellente della crittografia, è illegale ricercare come quella crittografia è usata. Ciò conduce alla vostra prima esercitazione:

1. Cosa è il "DeCSS" e come si riferisce alla cifratura dei DVD? Cercate "decss" per saperne di più.

2. Sapere che qualcosa è protetto da password significa imparare come aprire quel file. Ciò è conosciuto come "password cracking". Trovate le informazioni sul "cracking" di vari tipi di parole d'accesso. Per farlo cercate "cracking XYZ passwords" dove XYZ è il tipo di parola d'accesso che state cercando. Fatelo per i seguenti tipi di parola d'accesso:

a. MD5

b. Windows Administrator

c. Adobe PDF

d. Excel

3. Nel caso in cui il metodo di crittografia è troppo "robusto" per essere decifrato, può essere necessario realizzare un "dictionary attack" o "attacco del dizionario" (a volte conosciuto come "brute force"). Scoprite che cosa è un attacco del dizionario e cercate uno strumento per realizzarlo contro il file UNIX delle `password /etc/passwd` o `/etc/passwd/shadow`.

8.2.3 Trovare l'ago nel pagliaio

Il software forense commerciale include potenti strumenti di ricerca che permettono ricerche con molte combinazioni e permutazioni dei fattori. Senza questi costosi strumenti commerciali dovete dimostrare un po' più d'inventiva. Linux vi fornisce programmi di utilità standard che vi permettono di costruire strumenti simili a quelli commerciali. Il testo seguente illustra l'uso di **find**, **grep**, **string** e l'utilizzo di **pipe** per combinarli.

8.2.3.1 find

```
find [path...][expression]
```

find è usato individuare file che rispondono a determinati criteri di verifica all'interno del sistema operativo. Non è progettato per osservare all'interno dei file. Ci deve essere un milione di permutazioni delle espressioni che possono essere combinate per cercare un file.

Esercizio:

1. Leggete la pagina del manuale di find. Nella tabella che segue completate la colonna "Effetto" per ogni "Espressione". (suggerimento: Dove un numero compare come argomento, può essere specificato come segue: +n – per maggiore di n; - n - per di minore di n; n – uguale a n.)

Expression	Effect
-amin n	File last accessed n minutes ago
-anewer	
-atime	
-cnewer	
-iname	
-inum	
-name	
-regex	
-size	
-type	
-user	

8.2.3.2 grep

grep è uno strumento molto potente. È usato per trovare determinate linee all'interno di un file. Ciò vi permette di trovare rapidamente file che contengono determinate cose all'interno di una directory o di un file system. Ci sono modalità che permettono di specificare i criteri di verifica da abbinare alla ricerca. Per esempio: trovate tutte le stringhe nel dizionario che cominciano con la "s" e rifiniscono con la "a" per aiutare a compilare le parole incrociate.

```
grep ^s.*t$ /usr/share/dict/words
```

Esercizi:

1. Leggete le pagine del manuale di grep.
2. Cercate le "regular expressions" di grep su Internet. Cercate di costruire una "regular expression" che cerchi tutte le parole che sono lunghe quattro lettere e contengono una "a".

8.2.3.3 strings

strings è un altro programma utile. Esso cerca all'interno di un file di qualunque tipo le stringhe leggibili dall'uomo. Ciò può restituire moltissime informazioni su uno specifico file, fornendo spesso informazioni sull'applicazione che le ha generate, autori, data di creazione e così via.

Esercizio:

1. Leggete le pagine del manuale di strings.

8.2.3.4 awk

awk é un linguaggio di programmazione progettato per lavorare con le stringhe. E' utilizzato per estrarre informazione da un comando per fornire i parametri ad un altro. Per esempio, per evidenziare solo i programmi funzionanti dal comando ps, eseguite quanto segue:

```
ps | awk '{print $4}'
```

Esercizio:

1. Leggete le pagine del manuale di awk.

8.2.3.5 Pipe "|"

Tutti gli strumenti esaminati sono facilmente combinabili usando il comando "pipe" di UNIX, indicato con il simbolo "|". Ciò vi permette di prendere l'output di un comando e, per mezzo di pipe, di utilizzarlo come input di un altro. Per trovare tutte i file della directory corrente che sono di tipo mpg eseguite:

```
ls | grep mpg
```

Esercizi:

1. Utilizzate pipe, i comandi ls e grep e trovate tutti I file della directory corrente che sono stati creati questo mese.
2. Utilizzate il commando ps e awk, per generare la lista dei nomi di tutti i processi attivi.

8.2.4 Usare altre fonti

Ci sono molti altri metodi interessanti per esaminare com'é stato utilizzato un computer. Quasi ogni applicazione che va in esecuzione, oltre i file su cui agisce direttamente o che genera, registra alcuni dati supplementari. In particolare vi possono essere file temporanei utilizzati per l'elaborazione, la lista degli ultimi file utilizzati o la storia della navigazione di un browser web.

Esercizi

1. Che cosa è la cache del browser? Trovate dove il vostro web browser memorizza la cache.
2. Cosa sono i cookie? Trovate dove il vostro browser memorizza i cookie.
3. Cercate informazioni che riguardano i cookie. Che genere di cookie ci sono e che genere di informazioni memorizzano?
4. Il vostro computer usa per default delle directory temporanee in cui scrive i file per l'utente. Ciò è spesso noto come "Application data". Trovate le directory temporanee disponibili sul vostro PC. Aspettatevi di trovare tmp o temp, sovente ve ne sono più di quelle che conoscete. Cercare i file che sono stati modificati in data odierna, è il modo più efficace per trovare i file temporanei. I file temporanei spariscono quando si riavvia il PC?

8.3 Pratiche forensi di rete (network forensics)

8.3.0 Introduzione

Le pratiche forensi di rete o Network forensics sono utilizzate per scoprire dove si trova un computer e per dimostrare se un particolare file é stato inviato da un particolare computer Poiché le pratiche forensi di rete possono essere molto complicate ci occuperemo qui di alcuni principi base applicabili nel lavoro quotidiano.

8.3.1 Log dei firewall

Chi si collega al mio PC? Il firewall è un programma che può interrompere i collegamenti fra due punti in una rete. Esistono molti tipi di firewall. Indipendentemente dal tipo e dal lavoro svolto, i file di log dei firewall vi forniscono i dettagli. Soltanto usando i log, potete trovare le tracce degli attacchi e degli abusi subiti dal vostro firewall.

Esercizi

1. Visitate il sito http://www.dshield.org. Questo sito Web accetta i log dei firewall da tutto il mondo, è un tentativo di raccogliere i dati che si riferiscono alle attività dei cracker. Questi dati sono catalogati e ricapitolati e possono essere usati dai professionisti della sicurezza per verificare se le reti che devono proteggere sono vulnerabili a particolari attacchi, prima che avvengano. Visitate il sito e spiegate come sono stati costruiti i diagrammi a torta e cosa significano.

2. Sullo stesso sito leggete la sezione "Fight back" e i messaggi E-mail di risposta. Spiegate lo scopo.

8.3.2 Intestazioni dei messaggi di posta elettronica (Mail Headers)

I messaggi E-mail giungono con le informazioni di ogni calcolatore che attraversano per raggiungervi. Queste informazioni sono mantenute nelle intestazioni (headers). A volte negli header si trovano ancora più informazioni. Osservare le intestazioni tuttavia non è sempre così semplice. I vari client di posta hanno tutti modi differenti per mostrare gli header. Il segreto per leggere le intestazioni è sapere che sono in ordine inverso. La parte superiore della lista siete voi. Nell'ultima linea della lista vi è il computer da cui è partito il messaggio.

Esercizi

1. Una gran risorsa dedicata al network forensics per la lotta allo Spam è http://www.samspade.org. Visitate SamSpade.org e andate alla sezione chiamata "The library". Usando questa sezione dovreste potere spiegare come leggere le intestazioni dei messaggi E-mail. Dovreste anche cercare informazioni su "forged e-mail headers" e "e-mail abuse. Spiegate i vari modi con cui i messaggi E-mail possono essere usati per causare danno.

2. Stabilite come esaminare gli header dei messaggi E-mail che ricevete. Ci sono campi particolari che vi sembrano sconosciuti? Approfondendo, dovreste essere capaci di spiegare il significato d'ogni campo.

Successivi approfondimenti

I seguenti link sono in lingua inglese.

http://www.honeynet.org/papers/forensics/
http://www.honeynet.org/misc/chall.html - Alcuni esercizi forensi.
http://www.porcupine.org/forensics/ - I classici
http://www.computerforensics.net/
http://www.guidancesoftware.com/corporate/whitepapers/index.shtm#EFE
http://www.forensicfocus.com/
http://www.securityfocus.com/infocus/1679
http://www.linuxsecurity.com/feature_stories/feature_story-139.html
http://www.linuxsecurity.com/feature_stories/feature_story-140.html
http://www.securityfocus.com/incidents
http://staff.washington.edu/dittrich/talks/blackhat/blackhat/forensics.html
http://www.openforensics.org/
http://fire.dmzs.com/
http://www.sleuthkit.org/
http://www.fbi.gov/hq/lab/fsc/backissu/oct2000/computer.htm