DIGITAL FORENSICS

Corso di Sicurezza II

Dipartimento dI Informatica

Paolo Dal Checco

CHI SONO

- **Dottorato in Informatica**, gruppo di Sicurezza, @unito
- Per alcuni anni ricerca, poi **CTO** in ambito **crittografia**
- Ora **consulente Informatico Forense** per Procure, Tribunali, Aziende e Privati in ambito penale e civile
- Esperto di aspetti investigativi delle criptomonete, ransomware, computer/mobile/web/network forensics, perizie audio e video
- Tra i fondatori dell'Osservatorio Nazionale di Informatica Forense (**ONIF**), sviluppatore DEFT Linux fino al 2018
- Socio Tech & Law, Clusit, AIP, AssobIT
- paolo@dalchecco.it - @forensico
- dalchecco.it, bitcoinforensics.it, ransomware.it

PROGRAMMA PRIMA PARTE

- Introduzione alle problematiche di Computer Forensics
- Le fasi dell'accertamento forense su dati digitali
- Princìpi, preparazione, precauzioni e utilizzo dei sistemi Live
- Introduzione al sistema DEFT e DART
- Utilizzo di DEFT con i principali OS e filesystem

INTRODUZIONE ALLE PROBLEMATICHE DI COMPUTER FORENSICS

COS'È LA COMPUTER FORENSICS?

L'informatica forense è la scienza che studia, in ambito giuridico, l'individuazione, la conservazione, la protezione, l'estrazione, la documentazione, l'impiego ed ogni altra forma di trattamento del dato informatico al fine di essere valutato in un processo

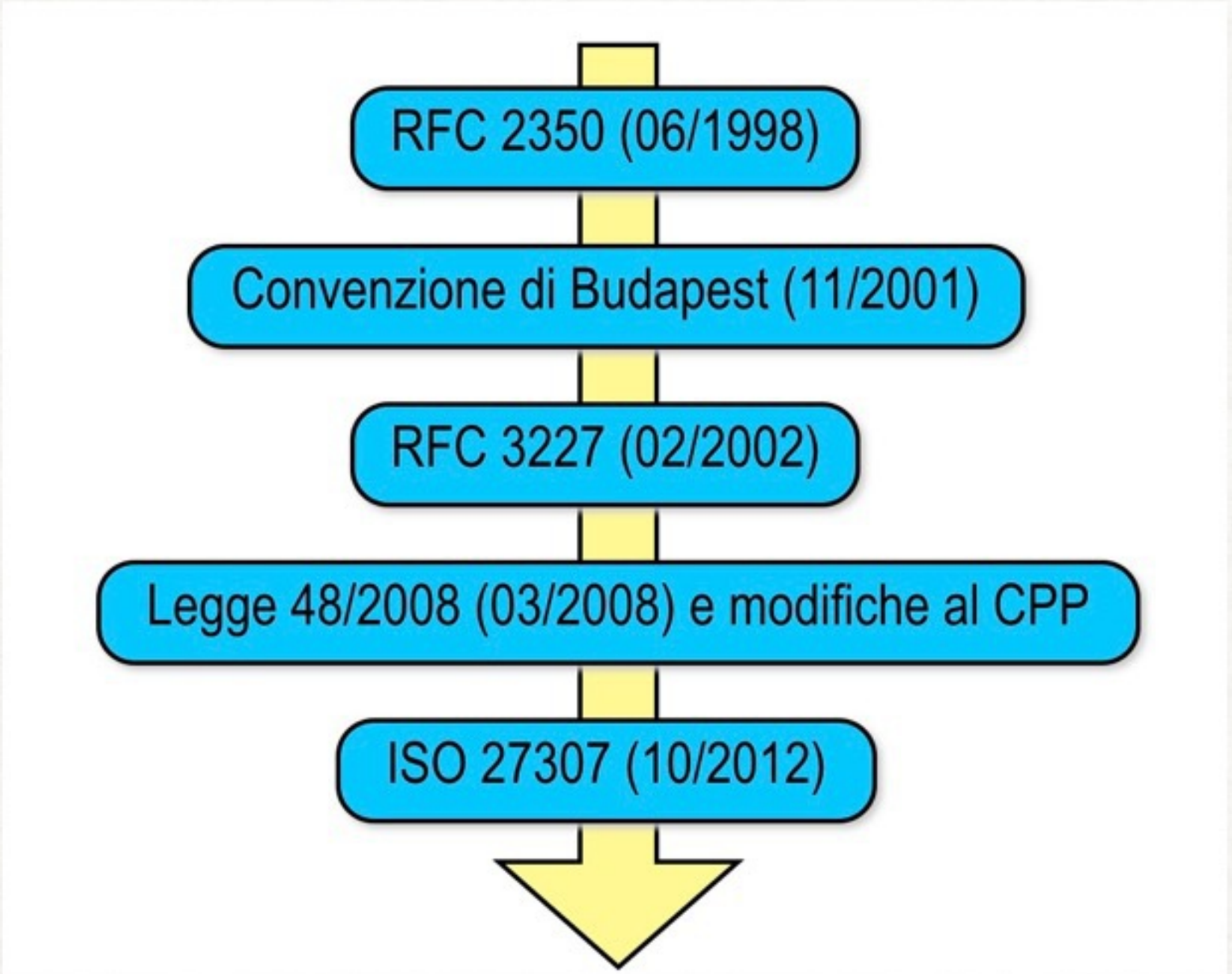
INTRODUZIONE ALLE PROBLEMATICHE DI COMPUTER FORENSICS

SCOPI DELLA COMPUTER FORENSICS

- Confermare o escludere un evento
- Individuare tracce e informazioni utili
- Acquisire e conservare le tracce in maniera idonea, che garantisca integrità e non ripudiabilità
- Interpretare e correlare le prove acquisite
- Documentare con precisione ed efficienza

INTRODUZIONE ALLE PROBLEMATICHE DI COMPUTER FORENSICS

NORMATIVE E BEST PRACTICES



INTRODUZIONE ALLE PROBLEMATICHE DI COMPUTER FORENSICS

- Operazioni ripetibili (art. 359 c.p.p.)
- Non bisogna alterare il reperto
- Documentare ogni operazione compiuta
- Documentare software e versioni usati
- Controllare lo se c'è uno sfasamento temporale
- Catena di custodia
- Utilizzare un write blocker o distribuzione forense (DEFT Linux)

INTRODUZIONE ALLE PROBLEMATICHE DI COMPUTER FORENSICS

BEST PRACTICES – L'INCIDENTE INFORMATICO (RFC 2350)

- Un evento che compromette aspetti della sicurezza dei computer e delle reti, con almeno uno dei seguenti fattori:
  - perdita di **confidenzialità** delle informazioni
  - compromissione dell'**integrità** delle informazioni
  - **interruzione** di servizio
  - **utilizzo inappropriato** di servizi, sistemi, informazioni
  - **danneggiamento** di sistemi
- Emerge l'mportanza del CSIRT "Computer Security Incident Response Team"

INTRODUZIONE ALLE PROBLEMATICHE DI COMPUTER FORENSICS

BEST PRACTICES – ACQUISIZIONE DELLE PROVE (RFC3227)

La RFC3227: Guidelines for Evidence Collection and Archiving

Pubblicata nel febbraio 2002, è ancora un punto di riferimento internazionale. Tra le altre cose consiglia di:

- Documentare dettagliatamente ogni operazione svolta (chiari riferimenti temporal indicando eventuali discrepanze)
- Evitare tecniche invasive o limitarne l'impatto, preferendo strumenti ben documentabili
- Isolare il sistema da fattori esterni che possono modificarlo (attenzione: l'attività potrebbe essere rilevata)
- Nella scelta tra acquisizione e analisi, **PRIMA** si acquisisce e **POI** si analizza
- Essere metodici e implementare automatismi (attenzione: arma a doppio taglio)
- Procedere dalle fonti più volatili alle meno volatili
- Eseguire copie bit-level (bit stream image) e lavorare su esse

INTRODUZIONE ALLE PROBLEMATICHE DI COMPUTER FORENSICS

- ISO **27037**: ""Guidelines for identification, collection, acquisition and preservation of digital evidence"
- La ISO/IEC 27037:2012 si limita alle fasi iniziali del processo di gestione della prova informatica, non arriva all'analisi, non si occupa di aspetti legali, strumenti, reportistica, trattamento dei dati
- Integrità della prova informatica e metodologia al fine di rendere ammissibile la prova in giudizio

- Si occupa di trattamento del reperto informatico e **identifica 4 fasi**:
  - 1)Identificazione (ispezione),
  - 2) Raccolta (sequestro)
  - 3) Acquisizione (copia o sequestro virtuale)
  - 4) Conservazione (conservazione e sigillo)

INTRODUZIONE ALLE PROBLEMATICHE DI COMPUTER FORENSICS

49016-17

In caso di diffusione del presente provvedimento omettere le generalità e gli altri dati identificativi, a norma dell'art. 52 d.lgs. n. 196/03 in quanto:
☐ disposto d'ufficio
☐ a richiesta di parte
☐ imposto dalla legge

REPUBBLICA ITALIANA

In nome del Popolo Italiano

LA CORTE SUPREMA DI CASSAZIONE

QUINTA SEZIONE PENALE

Composta da:

PUBBLICA UDIENZA
DEL 19/06/2017

MARIA VESSICHELLI - Presidente -
CATERINA MAZZITELLI
SERGIO GORJAN
GIUSEPPE DE MARZO
IRENE SCORDAMAGLIA - Rel. Consigliere -

Sent. n. sez.
1660/2017

REGISTRO GENERALE
N.9109/2017

http://www.processopenaleegiustizia.it/materiali/49016.pdf

INTRODUZIONE ALLE PROBLEMATICHE DI COMPUTER FORENSICS

2. Va giudicata ineccepibile la decisione della Corte territoriale di non acquisire la trascrizione delle conversazioni svoltesi sul canale informatico denominato '*whatsapp*', tra l'imputato e la parte offesa il 2 gennaio 2014, che la difesa dell'imputato avrebbe voluto versare agli atti del processo a riprova della inattendibilità della persona offesa, che aveva sostenuto che la relazione con l'imputato si era interrotta nell'ottobre 2013.

Deve, infatti, osservarsi che, per quanto la registrazione di tali conversazioni, operata da uno degli interlocutori, costituisca una forma di memorizzazione di un fatto storico, della quale si può certamente disporre legittimamente ai fini probatori, trattandosi di una prova documentale, atteso

INTRODUZIONE ALLE PROBLEMATICHE DI COMPUTER FORENSICS

l'utilizzabilità della stessa è, tuttavia, condizionata dall'acquisizione del supporto – telematico o figurativo - contenente la menzionata registrazione, svolgendo la relativa trascrizione una funzione meramente riproduttiva del contenuto della principale prova documentale (Sez. 2, n. 50986 del 06/10/2016, Rv. 268730; Sez. 5, n. 4287 del 29/09/2015 – dep. 2/02/2016, Pepi, Rv. 265624): tanto perché occorre controllare l'affidabilità della prova medesima mediante l'esame diretto del supporto onde verificare con certezza sia la paternità delle registrazioni sia l'attendibilità di quanto da esse documentato.

INTRODUZIONE ALLE PROBLEMATICHE DI COMPUTER FORENSICS

CONSIGLI UTILI

- Se il sistema è accesso, non spegnere il sistema prima di aver completato tutte le necessarie acquisizioni
- Valutare la modalità di spegnimento più idonea
- L'attaccante può aver alterato le normali procedure di shutdown
- Con uno spegnimento improvviso alcune informazione potrebbero andare perse
- Se il sistema è spento, non accenderlo
- Non fidarsi del sistema: utilizzare tool propri, compilati staticamente e su supporto in sola lettura
- Non usare programmi che possono alterare la timeline dei file
- La corretta profilazione dell'utente è importante per calibrare le modalità di intervento

INTRODUZIONE ALLE PROBLEMATICHE DI COMPUTER FORENSICS

CATENA DI CUSTODIA

Procedura che consente di tracciare lo stato di un reperto e la relativa responsabilità in qualsiasi momento della sua esistenza

Deve documentare in modo chiaro:

- Dove, quando e da chi il reperto è stato rinvenuto e acquisito
- Dove, quando e da chi è stato custodito e/o analizzato
- Chi ha avuto il reperto in custodia e in quale periodo
- Come è stato conservato
- Ad ogni passaggio di consegna, bisogna indicare dove e come è stato trasferito

Gli accessi ai reperti devono essere estremamente ristretti e documentati.

INTRODUZIONE ALLE PROBLEMATICHE DI COMPUTER FORENSICS

WRITE BLOCKER

- Il write blocker è un dispositivo hardware che:
  - Inibisce la scrittura sul dispositivo a cui è collegato in modo da non alterarlo
  - Fa credere al sistema operativo che ha accesso anche in scrittura (ma non è vero)
- Esistono anche write blocker software in particolare sono molto diffusi quelli per bloccare la scrittura su dispositivi USB

LE FASI DELL'ACCERTAMENTO FORENSE SU DATI DIGITALI

Il processo di investigazione forense prevede le seguenti fasi:

- Identificazione
- Preservazione
- Acquisizione
- Analisi
- Presentazione dei risultati

LE FASI DELL'ACCERTAMENTO FORENSE SU DATI DIGITALI

IDENTIFICAZIONE

- Individuare le informazioni o le fonti di informazione disponibili prestando attenzione in quanto i dati potrebbero essere nascosti (fisicamente o logicamente) oppure essere altrove

- Rilevare elementi ambientali può essere utile per reperire informazioni sugli usi e la disponibilità dei sistemi, soprattutto per individuare responsabilità personali

- Simili informazioni, se non annotate con precisione, potrebbero andar perse

- Potrebbe capitare che chi esegue l'acquisizione non è la stessa persona che effettuerà l'analisi

LE FASI DELL'ACCERTAMENTO FORENSE SU DATI DIGITALI

ALCUNE TIPOLOGIE DI MEDIA ACQUISIBILI

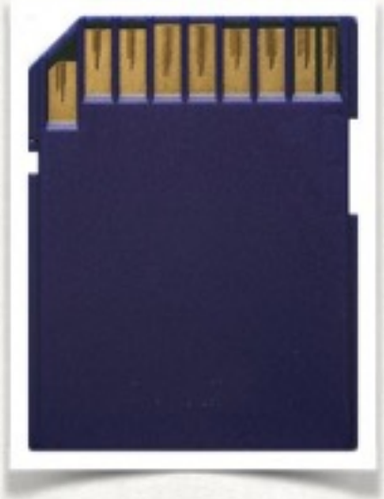
- Computer (hard disk interno)
- Dispositivi di storage comuni (hard disk esterni, chiavette USB, schede di memoria)
- Dispositivi di storage non comuni (orologi con memoria, coltellini svizzeri, ecc.)
- Floppy, CD, DVD o Blue-Ray
- Macchine fotografiche digitali
- Console
- Cellulari, Palmari, iPod, Smartphone, Tablet, Smartwatch

LE FASI DELL'ACCERTAMENTO FORENSE SU DATI DIGITALI

ALCUNE TIPOLOGIE DI MEDIA ACQUISIBILI

LE FASI DELL'ACCERTAMENTO FORENSE SU DATI DIGITALI

ALCUNE TIPOLOGIE DI MEDIA ACQUISIBILI



LE FASI DELL'ACCERTAMENTO FORENSE SU DATI DIGITALI

ALCUNE TIPOLOGIE DI MEDIA ACQUISIBILI

LE FASI DELL'ACCERTAMENTO FORENSE SU DATI DIGITALI

ALCUNE TIPOLOGIE DI MEDIA ACQUISIBILI

LE FASI DELL'ACCERTAMENTO FORENSE SU DATI DIGITALI

ALCUNE TIPOLOGIE DI MEDIA ACQUISIBILI

LE FASI DELL'ACCERTAMENTO FORENSE SU DATI DIGITALI

IDENTIFICAZIONE

Una volta identificato cosa acquisire bisogna:

- Saper valutare cosa va acquisito e cosa è trascurabile
- Essere in grado di acquisire tutto quello che è necessario
- "Etichettare" univocamente ogni supporto
- Assegnare un identificativo associato alla descrizione (marca, modello, seriale, ubicazione, stato ecc.)
- Stabilire il piano di acquisizione efficace

LE FASI DELL'ACCERTAMENTO FORENSE SU DATI DIGITALI

ACQUISIZIONE

Bisogna rispettare un ordine di volatilità:

- Registri, cache
- Memorie RAM
- Stato della rete (connessioni stabilite, socket in ascolto, applicazioni coinvolte, cache ARP, routing table, DNS cache ecc.)
- Processi attivi
- Memorie di massa (hard disk, pendrive USB, ecc.)
- Log remoti
- Floppy, nastri e altri dispositivi di backup
- Supporti ottici

LE FASI DELL'ACCERTAMENTO FORENSE SU DATI DIGITALI

ACQUISIZIONE

- Le copie eseguite devono essere identiche all'originale (integrità e non ripudiabilità)
- Le procedure devono essere documentate e attuate secondo metodi e tecnologie conosciute, così da essere verificabili dalla controparte

LE FASI DELL'ACCERTAMENTO FORENSE SU DATI DIGITALI

PRESERVAZIONE

- Non bisogna alterare il reperto originale (Write blocker / Distro Forense)

LE FASI DELL'ACCERTAMENTO FORENSE SU DATI DIGITALI

ANALISI

- Estrarre i dati e processarli per ricostruire informazioni
- Interpretare le informazioni per individuare elementi utili alle indagini
- Comprendere e correlare, in modo da affinare le ricerche e poterne trarre le conclusioni
- E' sicuramente la fase più laboriosa di tutto il processo e richiede conoscenze disparate

LE FASI DELL'ACCERTAMENTO FORENSE SU DATI DIGITALI

PRESENTAZIONE

Alla fine dell'attività di analisi, si deve presentare quanto elaborato, in una relazione tecnica:

- I risultati devono essere presentati in forma facilmente comprensibile a tutti
- I destinatari non hanno di solito competenze informatiche approfondite
- Tuttavia è probabile che la relazione venga esaminata da un tecnico della controparte
- Essere semplici e chiari, non bisogna essere superficiali e approssimati

PRINCÌPI, PREPARAZIONE, PRECAUZIONI E UTILIZZO DEI SISTEMI LIVE

- Un sistema live è un sistema operativo -DEFT Linux nel nostro caso- che per essere eseguito viene caricato nella memoria RAM in modo parziale o integrale (tramiteil parametro **toram**)
- NON scrive nulla sul disco rigido per poter essere eseguito
- Allo spegnimento del computer NON restano tracce del sistema live eseguito e le eventuali personalizzazioni al sistema verrano perse
- Un sistema live ad uso forense NON fa il mount automatico delle memorie di massa ad esso collegate

PRINCÌPI, PREPARAZIONE, PRECAUZIONI E UTILIZZO DEI SISTEMI LIVE

- Assicurarsi che venga fatto il boot da CD (o da USB) utilizzando gli appositi tasti (CANC, F2, F8, F12, ESC, ecc.) in modo da selezionare il corretto dispositivo di boot

- In caso contrario il boot verrebbe fatto dal sistema residente sull'hard disk con rischio di alterazione dei dati

- Nel caso di dubbio sul tasto di boot da utilizzare, scollegare temporaneamente il disco fisso a PC **SPENTO**

PRINCÌPI, PREPARAZIONE, PRECAUZIONI E UTILIZZO DEI SISTEMI LIVE

E' possibile selezionare tre modalità di avvio di DEFT:

- Utilizzando interfaccia grafica
- Tramite la modalità testuale utile nel caso in cui per qualsiasi motivo (es. risorse hardware limitare che non permettono l'avvio della GUI, scheda video non supportata, ecc.) non si possa utilizzare l'interfaccia grafica (è comunque possibile richiamare l'interfaccia grafica tramite il comando: **deft-gui**)
- Modalità "To RAM" passando il parametro **toram** in fase di boot (già presente nel menu di boot in DEFT Zero)
- Tramite interfaccia grafica è possibile montare in sola lettura le immagini o i dispositivi da analizzare direttamente utilizzando "Disk utility" o il file manager, mentre tramite interfaccia testuale bisogna prestare attenzione ad inserire l'opzione di "sola lettura" durante l'operazione di mount

INTRODUZIONE AL SISTEMA DEFT E DART

deft

Cos'è DEFT?

- Acronimo di Digital Evidence & Forensics Toolkit

- Nato nel 2005 in collaborazione con la cattedra del corso di Informatica Forense dell'Università degli studi di Bologna

- Dal 2007 diventa un progetto indipendente

- Nel settembre 2012 è nata l'associazione no profit per l'implementazione e lo sviluppo di DEFT e degli applicativi che lo compongono

- Il gruppo di sviluppatori si scioglie e l'associazione viene chiusa nel 2018, il progetto sta riassestandosi

INTRODUZIONE AL SISTEMA DEFT E DART

CHI USA DEFT?

BT

U.S. DEPARTMENT OF ENERGY

CID AGENT

FINECO
THE NEW BANK

THE DEPARTMENT OF THE TREASURY
1789

CARABINIERI

NEC RECISA RECEDIT

NASA

Polizia di Stato

POLITIET
ØSTFINNMARK POLITIDISTRIKT

INTRODUZIONE AL SISTEMA DEFT E DART

deft

- Distribuzione basata su Lubuntu Linux
- Deve essere avviata al boot via DVD o USB, ma può essere installata o eseguita in virtual machine (attenzione ala protezione dei dispositivi attraverso la VM)
- Ideale per eseguire copie forensi o triage
- Toolkit per acquisizione e analisi (timeline, metadati, supertimeline, registro, ecc.)

INTRODUZIONE AL SISTEMA DEFT E DART

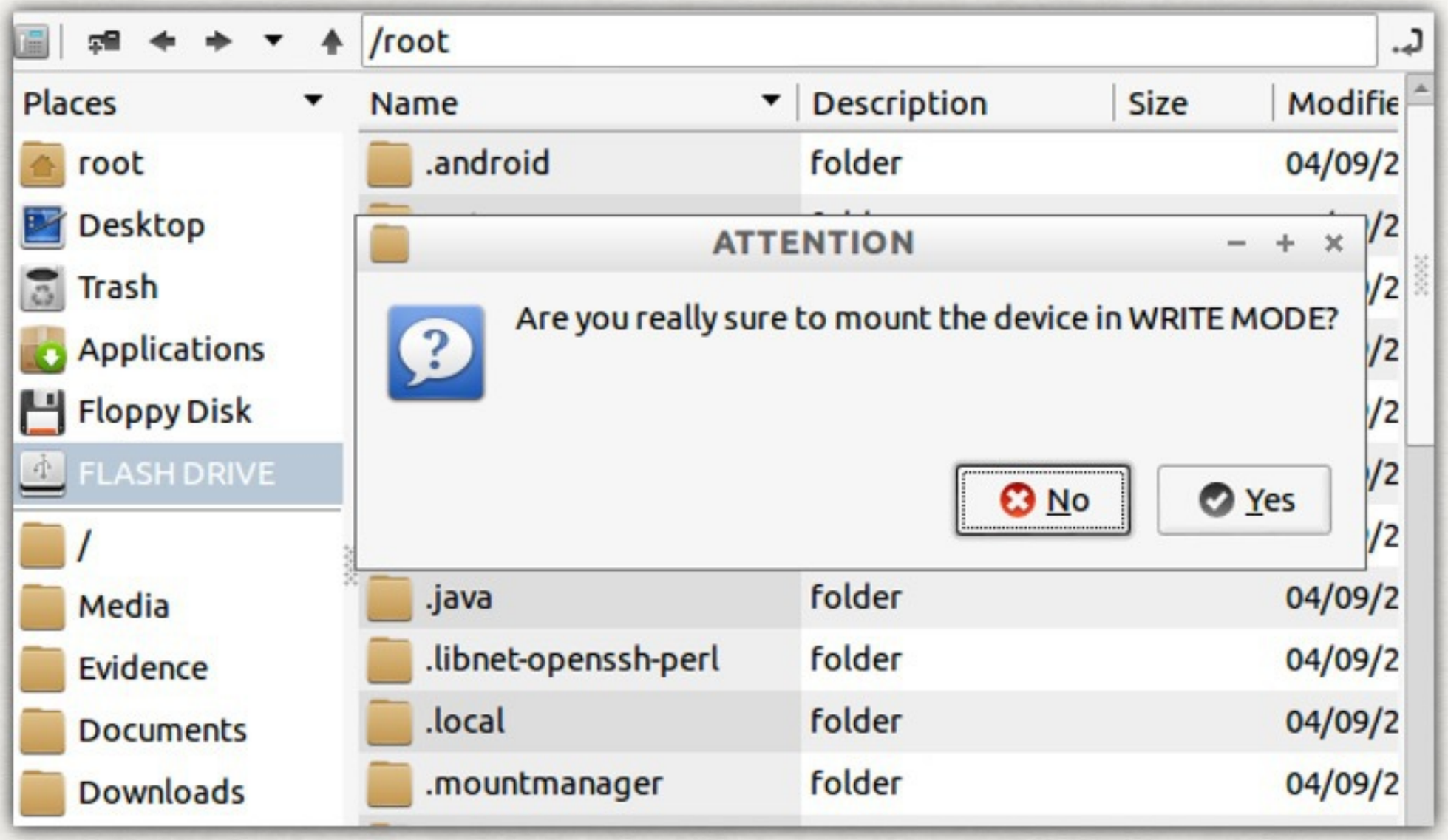
deft

- The Sleuthkit 
- Digital Forensics Framework DFF
- Implementato il supporto a Bitlocker - libbde
- Mobile Forensics, Android & iOS  iOS
- Skype Extractor 
- Osint Browser
- Maltego  MALTEGO
- Centinaia di altri tool

INTRODUZIONE AL SISTEMA DEFT E DART

deft

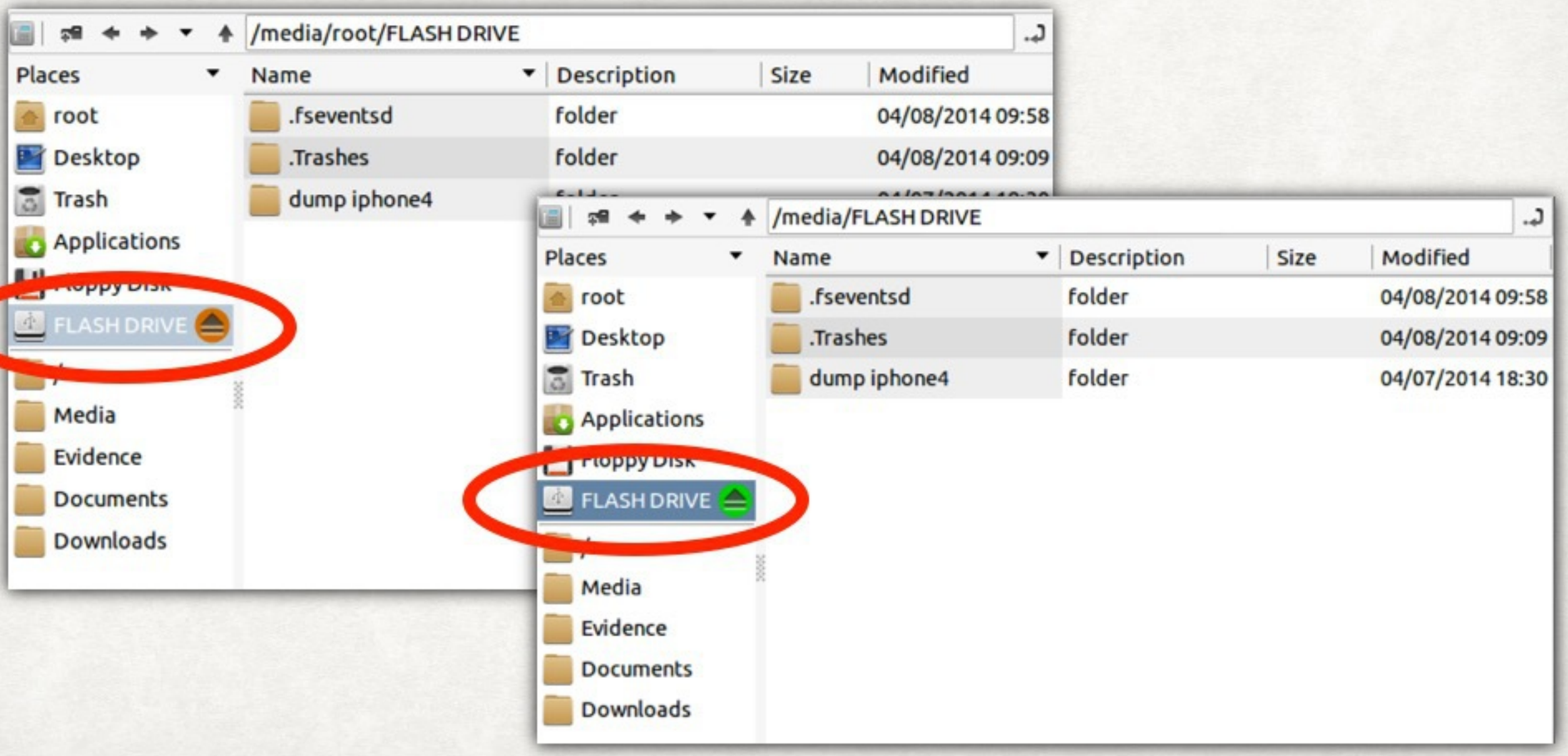
Mount dei dispositivi in sola lettura



INTRODUZIONE AL SISTEMA DEFT E DART

deft

Mount dei dispositivi in sola lettura



INTRODUZIONE AL SISTEMA DEFT E DART

deft zero

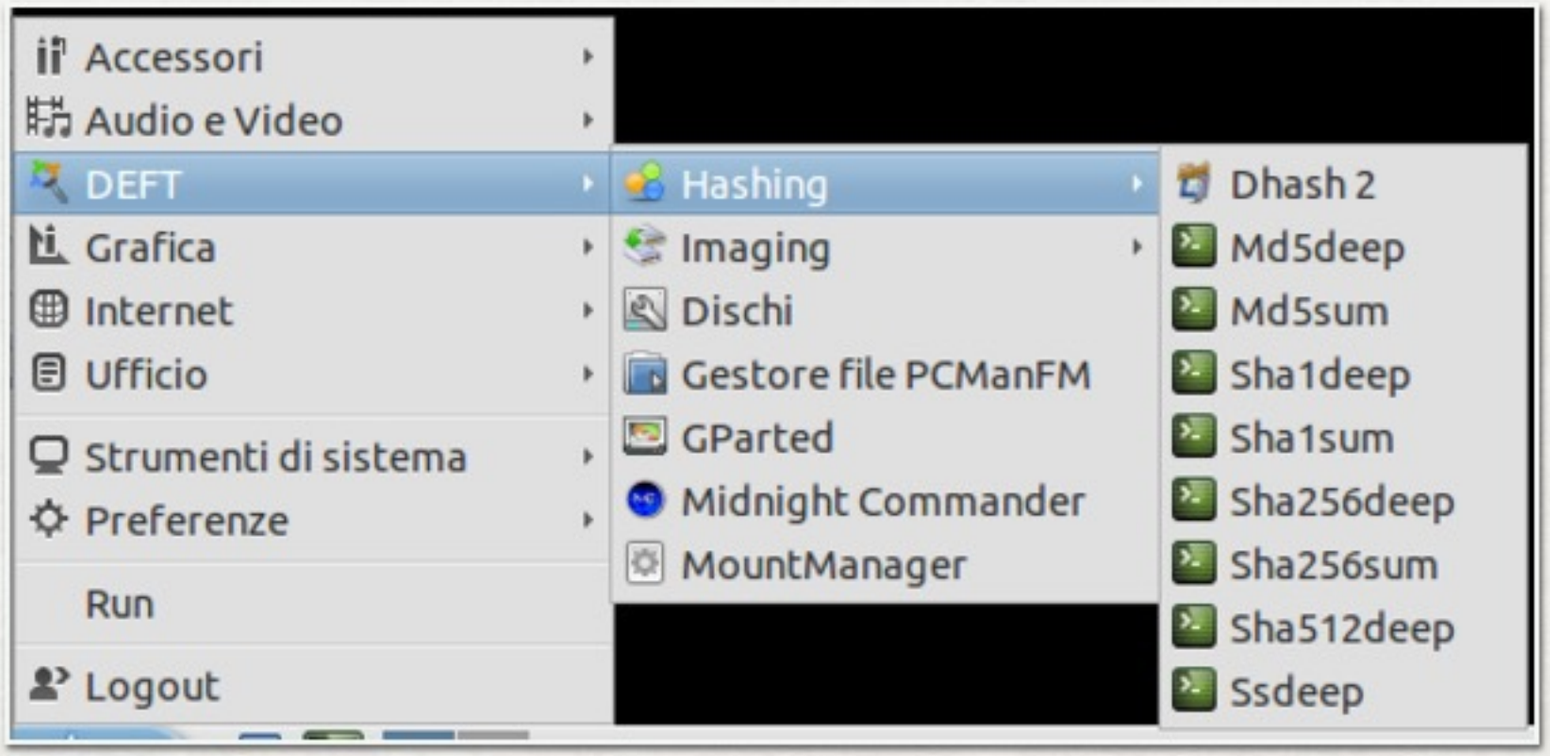
SUGAR FREE

- Basata su Lubuntu 14.04 **x86**
- La solidità di DEFT 8 in circa 400 MB di ISO
- Ottimizzato per le sole acquisizioni
  - Guymager, command line tool

INTRODUZIONE AL SISTEMA DEFT E DART

deft zero

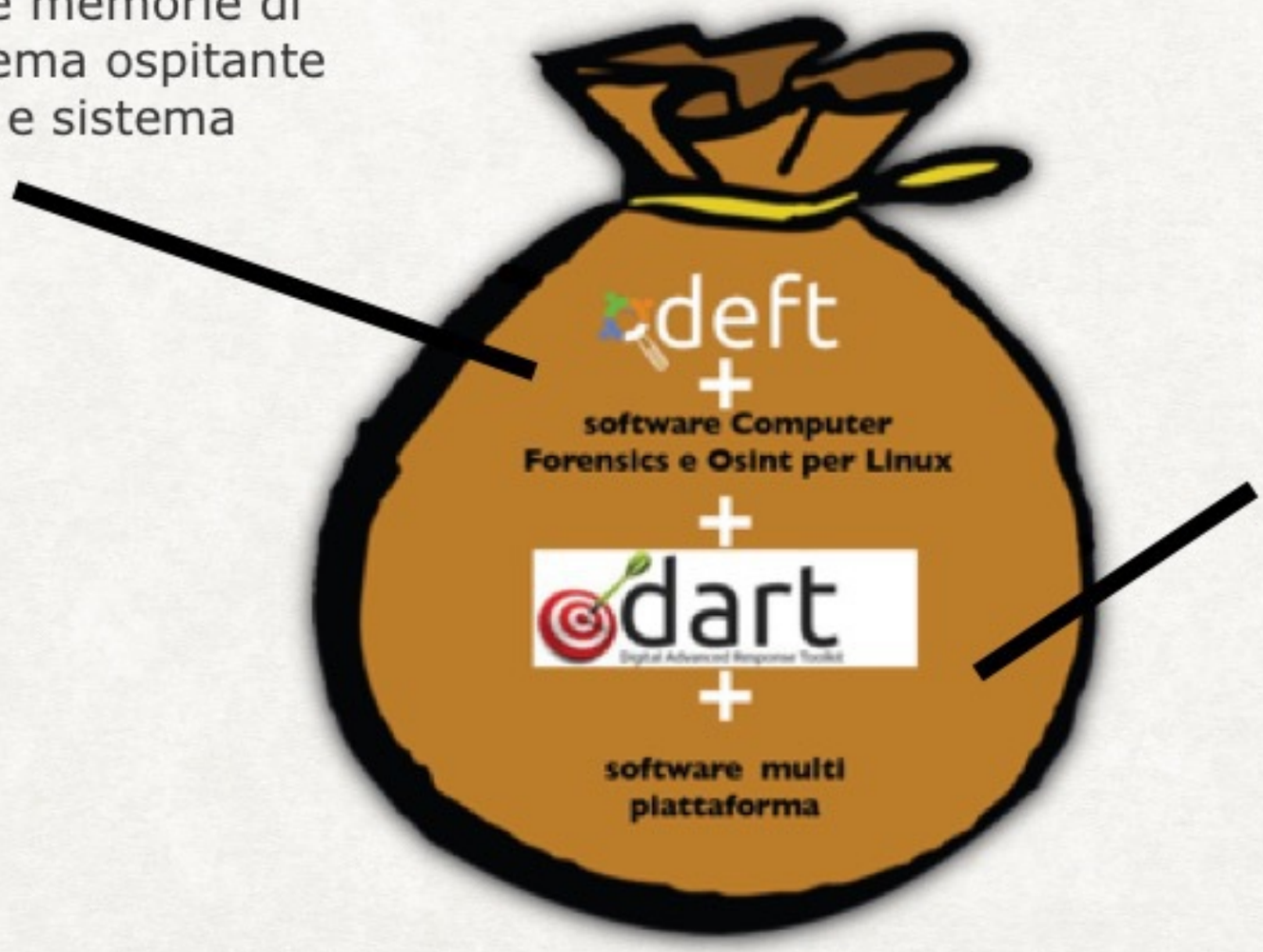
SUGAR FREE



INTRODUZIONE AL SISTEMA DEFT E DART

DEFT COME SOLUTION BAG

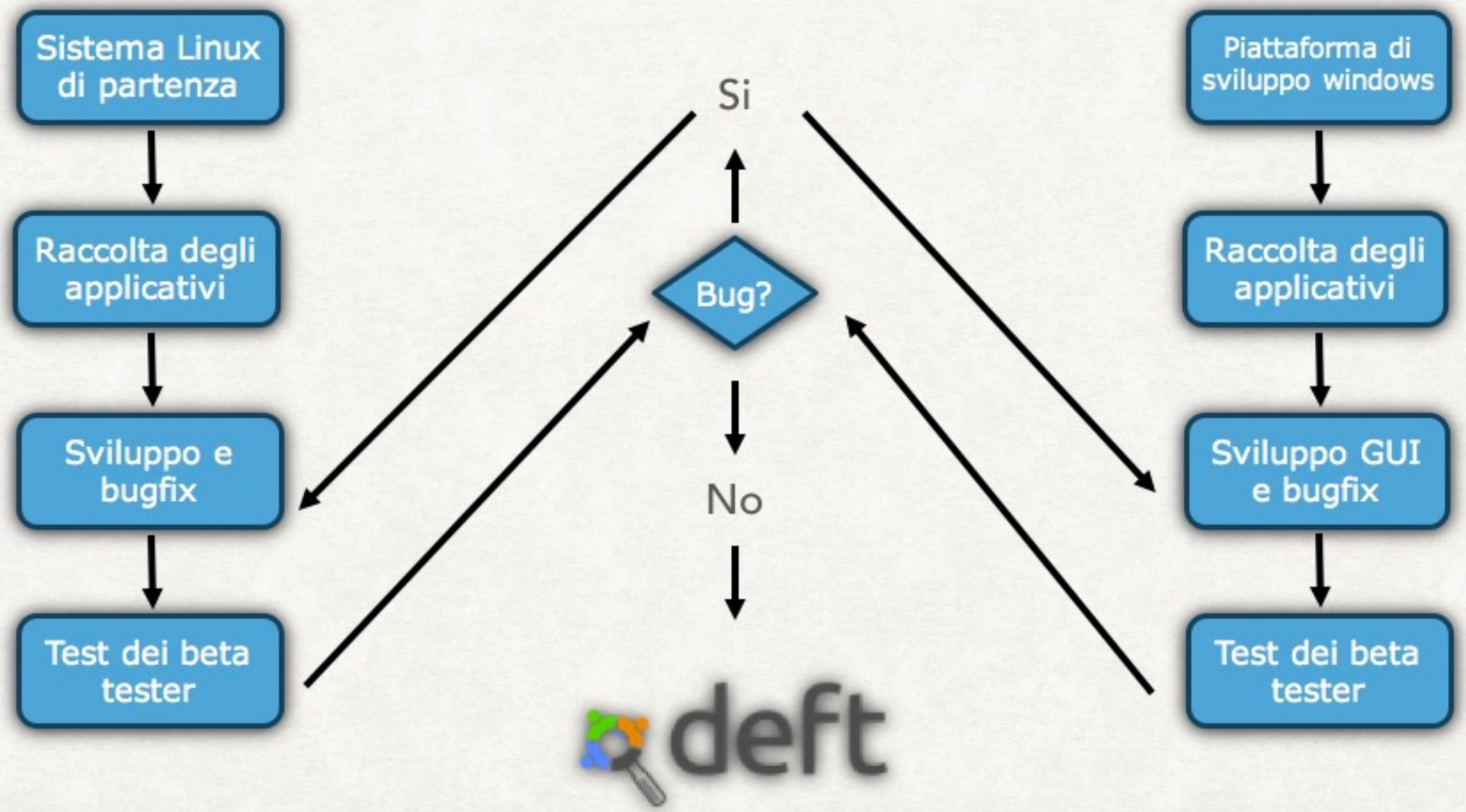
Sistema Linux live che mantiene inalterato il contenuto delle memorie di massa del sistema ospitante (ma anche VM e sistema installabile)



Interfaccia grafica multi piattaforma per attività di Incident Response
e Live Forensics

INTRODUZIONE AL SISTEMA DEFT E DART

LE FASI DELLO SVILUPPO



INTRODUZIONE AL SISTEMA DEFT E DART

DOVE È POSSIBILE USARE DEFT?

DEFT Linux: su tutte le architetture x86
dalla versione 8 su architetture a 64 bit

DART: su tutti i computer con Microsoft Windows
...ma non solo

INTRODUZIONE AL SISTEMA DEFT E DART

QUANDO PUÒ ESSERE UTILE?

Clonare un hard disk senza dover smontare lo schermo

INTRODUZIONE AL SISTEMA DEFT E DART

DOVE NON POSSO USARE DEFT?

Mainframe

Architetture non x86

INTRODUZIONE AL SISTEMA DEFT E DART

OLTRE ALLE ACQUISIZIONI?

- Analisi di memorie di massa
- Analisi di traffico di rete
- Analisi di dispositivi mobile
- Analisi di backup di iPhone e Black Berry
- Analisi dei database che compongono parte della app, sia per iOS che per Android
- Incident Response e Live Forensics
- Attività di analisi in contesti di Cyber Intelligence
- Organizzazione delle evidence

INTRODUZIONE AL SISTEMA DEFT E DART

DEFT IN MACCHINA VIRTUALE: VANTAGGI E SVANTAGGI

- DEFT mette a disposizione una virtual appliance, scaricabile dal sito ufficiale, già pronta per essere eseguita in una macchina virtuale

- DEFT infatti può essere utilizzato come un sistema per workstation atte all'analisi

INTRODUZIONE AL SISTEMA DEFT E DART

DEFT IN MACCHINA VIRTUALE: VANTAGGI E SVANTAGGI

Vantaggi:

- Non si necessita di una macchina fisica dedicata
- Sulla stessa macchina fisica è possibile installare più macchina per l'analisi (se l'hardware lo permette)
- Possibilità di aggiungere software
- Possibilità di salvare le personalizzazioni in modo persistente
- Possibilità di spostare il sistema virtualizzato da una macchina fisica all'altra
- Possibilità di condividere i file tra host e guest (anche diversi) ed eventualmente tra le varie macchine virtuali

INTRODUZIONE AL SISTEMA DEFT E DART

DEFT IN MACCHINA VIRTUALE: VANTAGGI E SVANTAGGI

Svantaggi:

- Necessita di hardware performante
- Il sistema host potrebbe scrivere su un eventuale device collegato per essere analizzato o acquisito (necessario write blocker), ma di ma solitamente non si collegano mai in questa modalità i device da acquisire

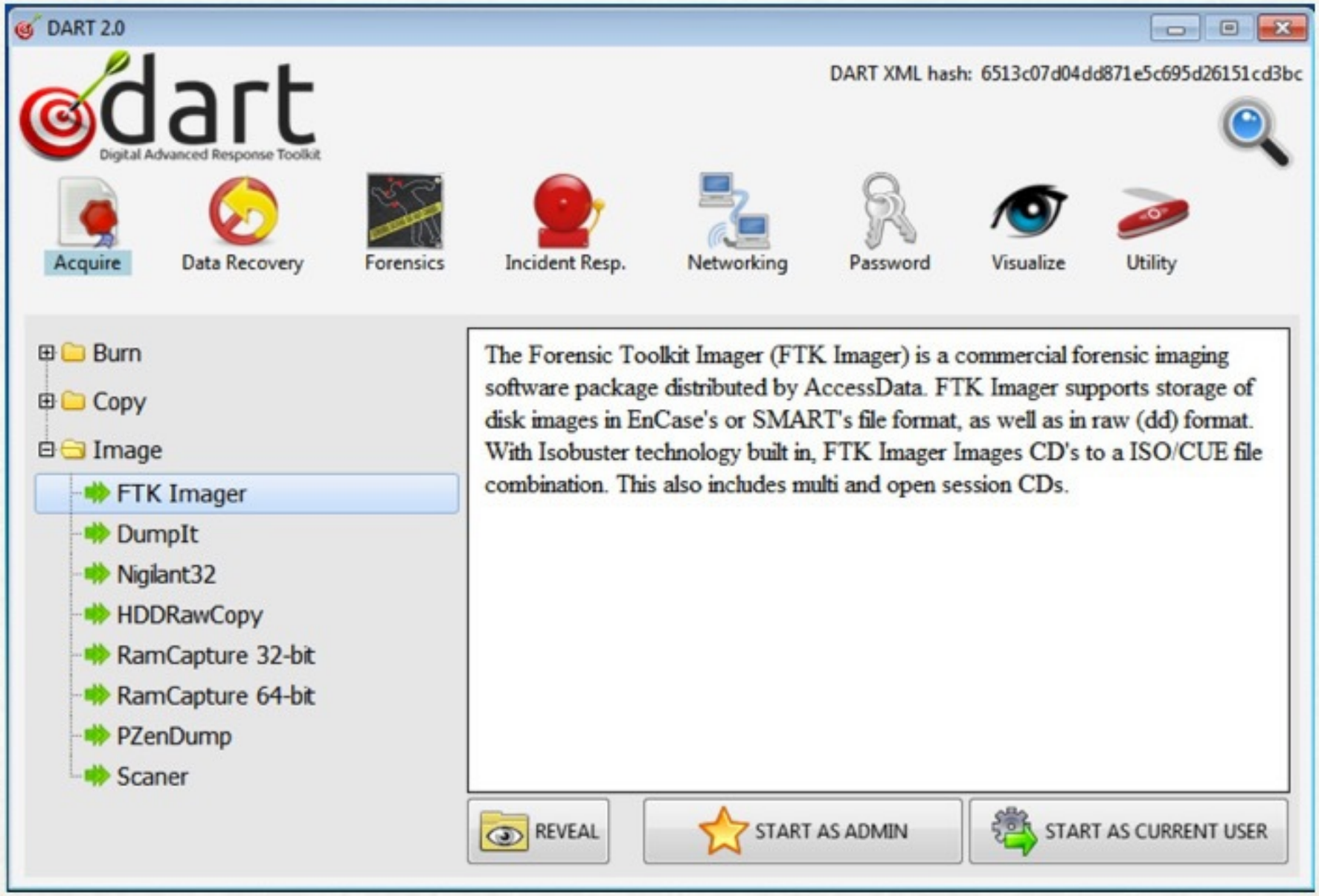
INTRODUZIONE AL SISTEMA DEFT E DART

Acronimo di Digital Advanced Response Toolkit

- Raccolta di applicativi ottimizzati, liberamente re-distribuibili per licenza d'uso, per eseguire attività di Incident Response e Live Forensics
- Alto livello di personalizzazione, senza l'obbligo di ricompilare codice sorgente
- Controllo dell'integrità dell'applicativo prima dell'avvio
- Binari dei principali sistemi operativi Windows, Linux e OS X

INTRODUZIONE AL SISTEMA DEFT E DART

DART



INTRODUZIONE AL SISTEMA DEFT E DART

DART: POTENZIALITÀ

- Acquisizione memorie di massa
- Dump memoria RAM
- Calcolo di hash
- Analisi processi
- Analisi traffico di rete
- Analisi registro di Windows
- Antimalware e antirootkit
- Time line degli eventi del sistema
- Analisi navigazione internet e posta elettronica
- Password cracking
- E molto altro...

UTILIZZO DI DEFT CON I PRINCIPALI O.S. E FILESYSTEM

MICROSOFT WINDOWS

- Il sistema operativo Windows 1.0 di Microsoft viene sviluppato per la prima volta nel 1985, era molto immaturo e non aveva il supporto per le reti.
- Vengono rilasciate nuove versioni fino ad arrivare alla attuale versione 10: progressivamente si introducono nuove feature e le varie versioni diventano sempre più affidabili
- Ricordiamo alcune feature:
  Obbligo utilizzo filesystem NTFS (da Windows XP)
  Active Directory
  Windows Update
  Multiutenza
  Disponibile per architetture a 64-bit (Win XP / più diffusamente con Vista)
  Bitlocker
  …

UTILIZZO DI DEFT CON I PRINCIPALI O.S. E FILESYSTEM

MS WINDOWS: CARTELLE DI INTERESSE

- La cartella utente:
  - **C:\Document and settings\NOME-UTENTE** (Win XP/Vista)
  - **C:\Users\NOME-UTENTE** (da Win 7)
  - NOTA: Nella cartella utente troviamo anche il file **NTUSER.DAT** che contiene i dati del registro relativi all'utente
    Inoltre fare riferimento alle altre sotto cartelle, le quali possono contenere altri file utili.
- Cartella con file del registro configurazione:
  - **C:\Windows\System32\Config**
- Cartella con il registro eventi:
  - **C:\Windows\System32\Config\Events**

UTILIZZO DI DEFT CON I PRINCIPALI O.S. E FILESYSTEM

MS WINDOWS: ALTRI PUNTI INTERESSANTI DEL SISTEMA

- Registro di sistema
- File di swap e di ibernazione (pagefile.sys, hiberfil.sys)
- Eventi di sistema (estensione .evt relativi a: Applicazione, Protezione, Sistema, …)
- Cestino, file recenti, thumbs.db, spooler di stampa
- Punti di ripristino
- Dati applicazioni e Impostazioni locali (Browser, e-mail, chat, software P2P)

UTILIZZO DI DEFT CON I PRINCIPALI O.S. E FILESYSTEM

LINUX

- Il sistema operativo GNU/Linux nasce nel 1991 partendo da un'idea di Linus Torvalds
- Sistema basato su Kernel "Unix-like" open source e gratuito
- Nascono le prime aziende e progetti senza scopo di lucro tra cui Red Hat, SuSe, Mandrake, Slackware, Debian, ecc.
- Arrivando ai giorni nostri, cresce il numero di distribuzioni. Nascono, muoiono diversi progetti, interessante è la distribuzione Ubuntu (e le sue derivate), sulla quale si base DEFT Linux

UTILIZZO DI DEFT CON I PRINCIPALI O.S. E FILESYSTEM

LINUX: CARTELLE DI INTERESSE

Il sistema Linux utilizza standard per i file e le cartelle (LSB) ma in alcuni sistemi si hanno delle piccole differenze. In ogni caso, possiamo fare riferimento a quanto segue:

- Cartella utente: **/home/NOME-UTENTE**
- Cartella con i log di sistema: **/var/log**
- Cartella con le configurazioni di sistema: **/etc**
  In questa cartella troviamo le varie configurazioni tra cui le impostazioni di rete, impostazioni globali del terminale ed altre configurazioni varie, tra cui il file con le password di sistema

Prestiamo particolare attenzione ai "file nascosti" in Linux iniziano con il carattere "." se accediamo a questo filesystem da un sistema Linux che ha disabilitato la visualizzazione dei file nascosti, NON saranno mostrati a video

UTILIZZO DI DEFT CON I PRINCIPALI O.S. E FILESYSTEM

LINUX: ALTRI PUNTI INTERESSANTI DEL SISTEMA

- Generalmente la struttura del filesystem è ordinata come segue:

  /bin contiene i file binari comuni
  /boot contiene il kernel e i file di avvio
  /dev contiene la mappatura dei device
  /etc contiene il i file di configurazione del sistema
  /home contiene i profili utente
  /mnt o **/media** contiene i punti di mount
  /root contiene il profilo dell'amministratore
  /sbin contiene i binari riservati a root
  /tmp contiene il i file temporanei
  /usr contiene gli applicativi non di sistema
  /var contiene i dati degli applicativi (log, mail, spool di stampa, database, sorgenti web, ecc.)

- Il filesystem può essere distribuito su più partizioni

UTILIZZO DI DEFT CON I PRINCIPALI O.S. E FILESYSTEM

LINUX: ALTRI PUNTI INTERESSANTI DEL SISTEMA

Non dimentichiamo che:

- La partizione di swap può contenere dati interessanti
- Le shell mantengono una history: **/home/NOME-UTENTE/.bash_history**
- Nella cartella /home dell'utente dobbiamo controllare:
    - Configurazioni personali
    - Dati delle applicazioni dell'utente
    - Dati dell'utente
    - Ricordandoci che generalmente i file o le cartelle contenenti le configurazioni iniziano con il carattere "." (es. ~/.config)

UTILIZZO DI DEFT CON I PRINCIPALI O.S. E FILESYSTEM

APPLE MAC OS

- Il sistema operativo Mac OS di Apple nasce nel 1984, il nome è l'acronimo di Macintosh Operating System
- Aveva la caratteristica di essere un sistema operativo completamente grafico. Questa novità favorì molto la popolarità delle GUI
- L'attuale Mac OS X ("10" in numeri romani) è stato completamente riscritto e migliorato (commercializzato dal 2001)

UTILIZZO DI DEFT CON I PRINCIPALI O.S. E FILESYSTEM

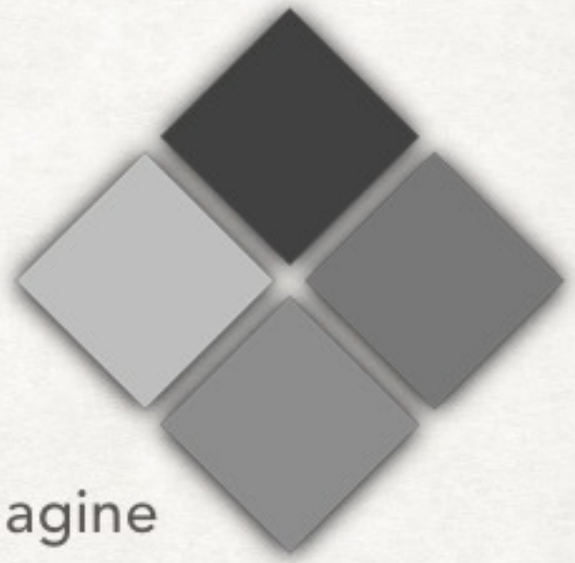
APPLE MAC OS X: CARTELLE DI INTERESSE

Le principali cartelle di interesse di OS X sono le seguenti:

- Cartella utente: **/Users/NOME-UTENTE**
- Cartella con i log di sistema: **/var/log**
- Cartella con le configurazioni di sistema: **/etc**
- Anche in questo caso, prestiamo particolare attenzione ai "file nascosti" in Linux iniziano con il carattere "." se accediamo a questo filesystem da un sistema Linux che ha disabilitato la visualizzazione dei file nascosti, NON saranno mostrati a video

UTILIZZO DI DEFT CON I PRINCIPALI O.S. E FILESYSTEM

APPLE MAC OS X: BOOT CAMP



Boot Camp è una tecnologia sviluppata da Apple che consente di installare un sistema Windows o Linux in una partizione del disco Macintosh. Il partizionamento avviene in modo non distruttivo e contestualmente viene fornito un immagine CD con i driver per far funzionare il sistema Windows installato

- Non dimentichiamo di verificare la presenza di tale partizione ed in caso positivo di fare un'analisi anche di quest'area

UTILIZZO DI DEFT CON I PRINCIPALI O.S. E FILESYSTEM

CARTELLE DI INTERESSE

Le cartelle indicate in precedenza sono cartelle particolari che potrebbero fornire materiale di interesse, tuttavia **NON** dobbiamo focalizzarci solo su queste, ma prendere una visione completa di tutto il sistema

UTILIZZO DI DEFT CON I PRINCIPALI O.S. E FILESYSTEM

COS'È UN FILESYSTEM?

In informatica, un file system è il metodo con il quale i file sono immagazzinati e organizzati su un dispositivo di archiviazione, come ad esempio un hard disk, una pendrive o un CD-ROM.

Più formalmente, un file system è l'insieme dei tipi di dati astratti necessari per la memorizzazione, l'organizzazione gerarchica, la manipolazione, la navigazione, l'accesso e la lettura dei dati.

UTILIZZO DI DEFT CON I PRINCIPALI O.S. E FILESYSTEM

COS'È UN FILESYSTEM?

I file system generalmente usano dispositivi di archiviazione che offrono l'accesso ad un array di blocchi di dimensione fissa, generalmente in settori di 512 byte l'uno.

Il file system è responsabile dell'organizzazione di questi settori e tiene traccia di quali settori appartengono a quali file, e quali invece non sono utilizzati.

UTILIZZO DI DEFT CON I PRINCIPALI O.S. E FILESYSTEM

TIPI DI FILESYSTEM

- Amiga FileSystems - OFS, FFS1 e 2, International, PFS, SFS usati su Amiga
- BFS (Beos File System) - file system nativo di BeOS
- DFS , ADFS - file system della Acorn
- EFS (IRIX) - un vecchio file system a blocchi usato su IRIX
- Ext2 - Extended File System 2, diffuso su sistemi GNU/Linux
- Ext3/Ext4 - Extended File System 3, diffuso su sistemi GNU/Linux (ext2+journaling)
- FAT - Usato su DOS, Microsoft Windows e su molti dispositivi dedicati, dispone di tabelle a 12 e 16 bit
- FAT32 - versione con tabelle a 32 bit di FAT
- FFS - Fast File System, usato in vecchi sistemi BSD
- HFS - Hierarchal File System, usato su vecchie versioni di Mac OS
- HFS+ - Hierarchal File System Plus, usato su Mac OS X

UTILIZZO DI DEFT CON I PRINCIPALI O.S. E FILESYSTEM

TIPI DI FILESYSTEM

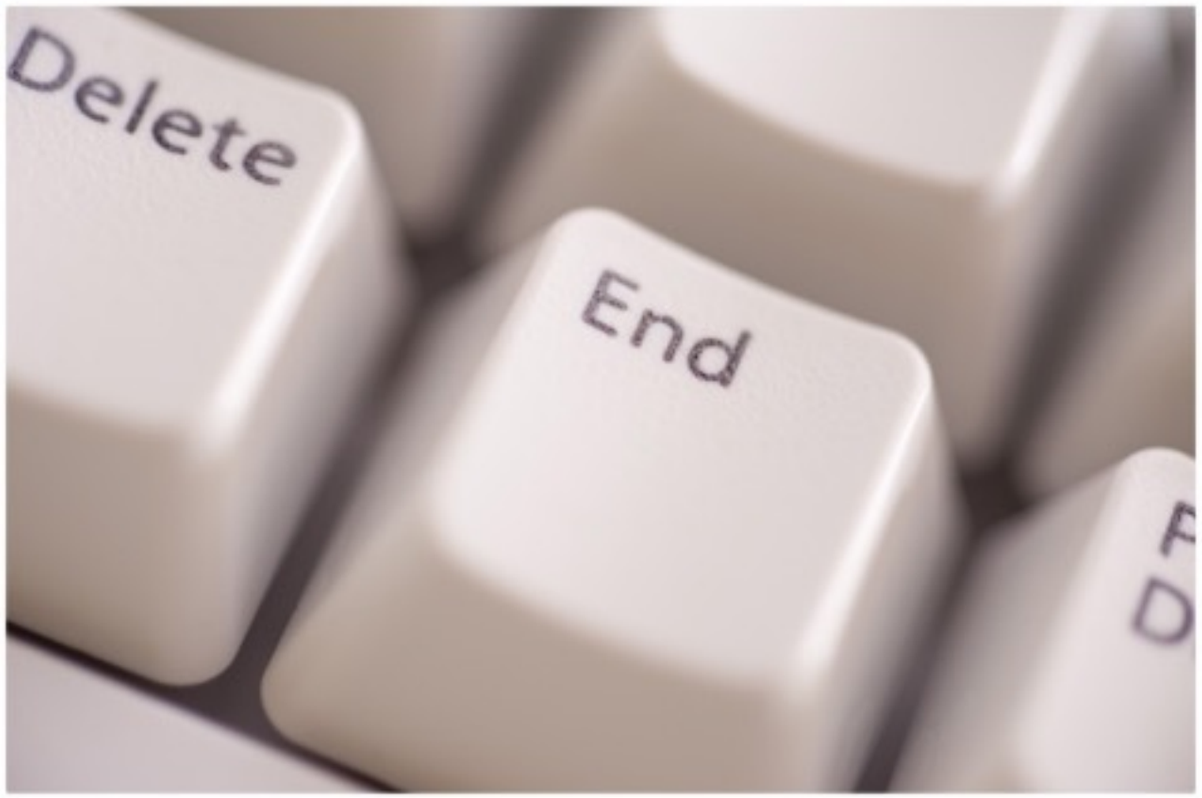
- HPFS - High Performance File System, usato su OS/2
- ISO 9660 - Usato su dischi CD-ROM e DVD-ROM (anche con estensioni Rock Ridge e Joliet)
- JFS - Journaling File System, disponibile su sistemi GNU/Linux, OS/2, e AIX
- LFS - Log-structured File System
- Minix - Usato su sistemi Minix
- NTFS - New Technology File System. Usato su sistemi Windows (NT, 2000, XP, Vista, 7, 8, 10)
- ReiserFS - File system journaling diffuso su sistemi GNU/Linux
- UDF - File system a pacchetti usato su supporti WORM/RW, CD-RW e DVD
- UFS/UFS2 - Unix File System, usato su vecchi sistemi BSD
- UMSDOS - File system FAT esteso con permessi e metadata, usato su GNU/Linux
XFS - Usato su sistemi IRIX
- ZFS - Creato dalla Sun

UTILIZZO DI DEFT CON I PRINCIPALI O.S. E FILESYSTEM

NETWORK FILESYSTEM

- AFS (Andrew File System)
- AppleShare
- CIFS (conosciuto anche come SMB o Samba)
- Coda
- GFS
- InterMezzo
- Lustre
- NFS

GRAZIE PER L'ATTENZIONE



LABORATORIO