COMPUTER FORENSICS

Lezione 21: L'Analisi
i sistemi operativi

A.A. 2021/22

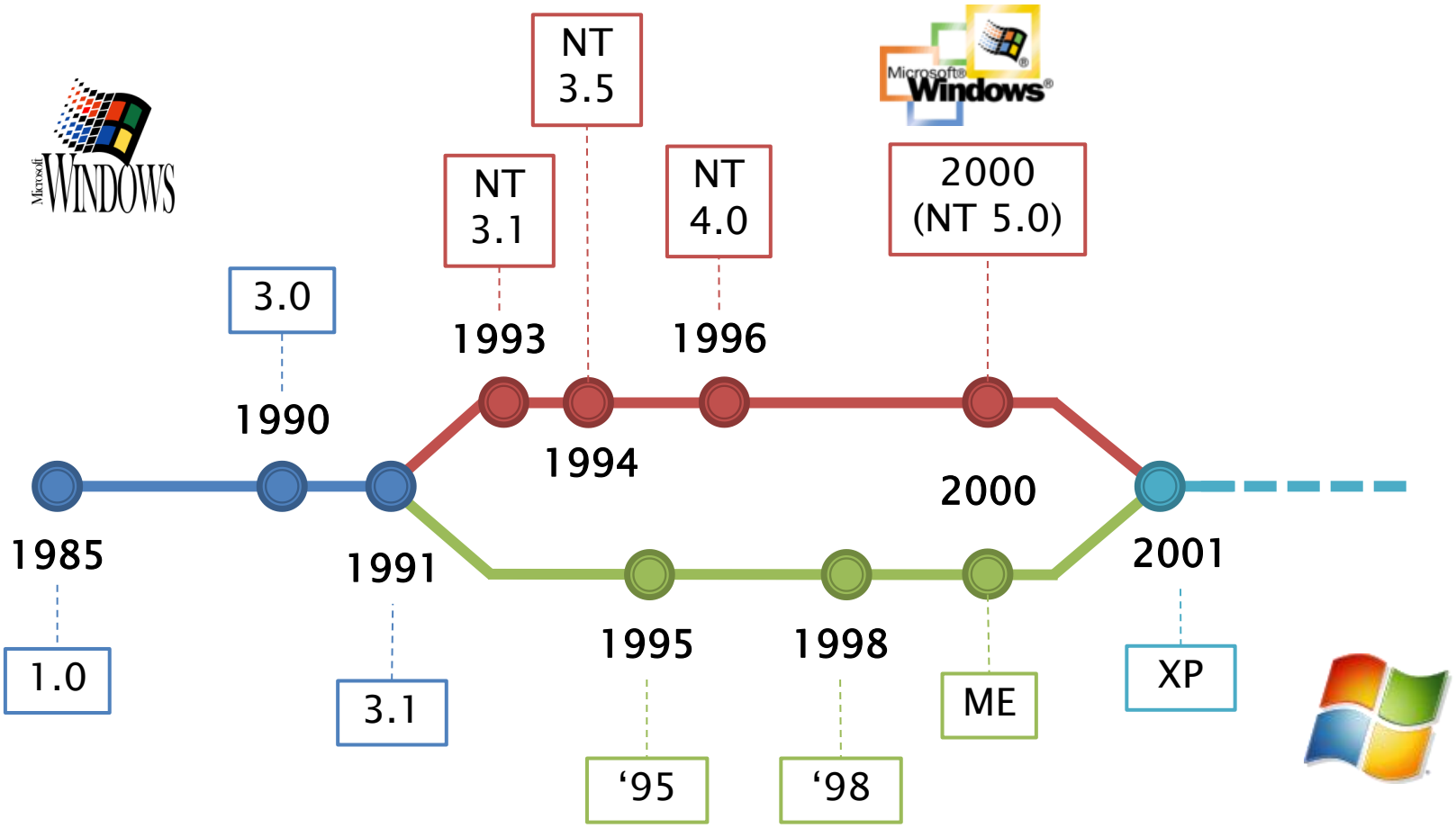
Dott. Lorenzo LAURATO

Sistemi Operativi

- Microsoft Windows

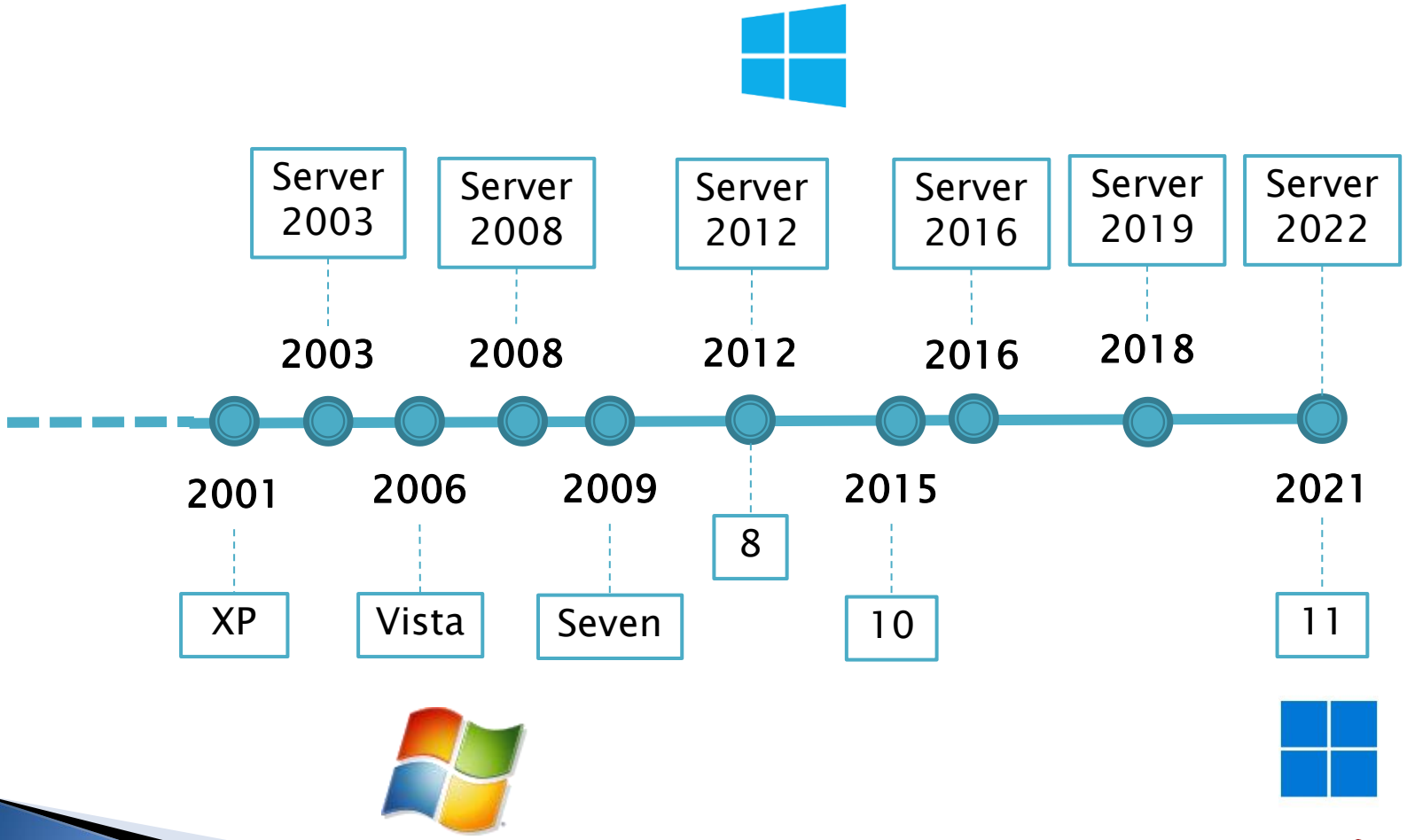
Microsoft Windows

storia



Microsoft Windows

storia



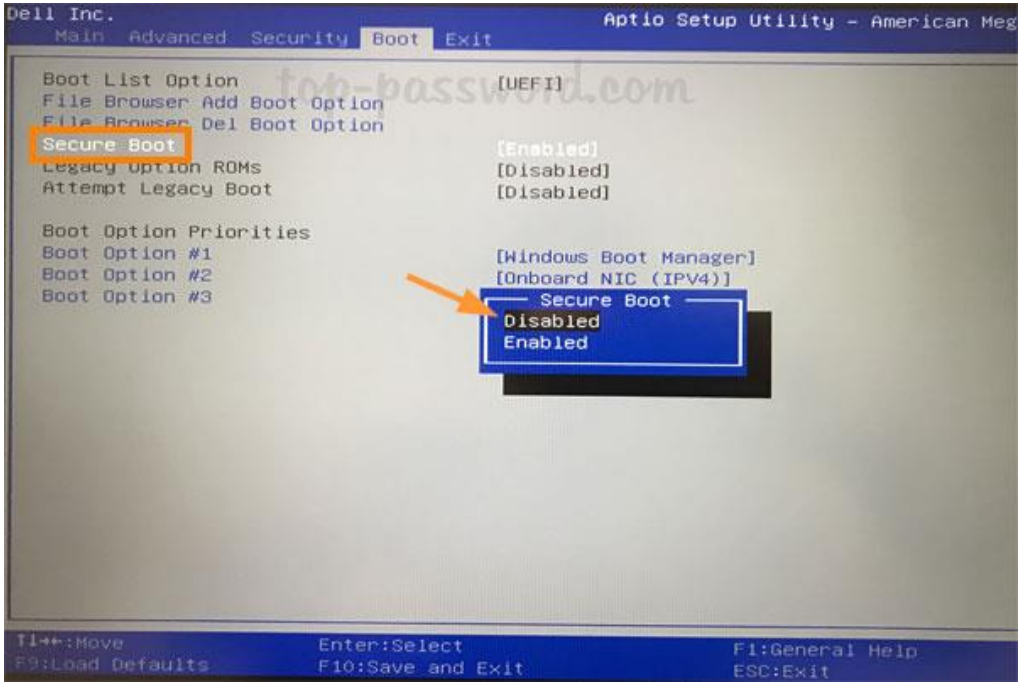
Microsoft Windows

users

- **Account locali**:
  - accesso al singolo sistema
  - autenticazione locale
- **Account di dominio**:
  - accesso a tutti sistemi attestati
  - autenticazione tramite Domain Controller
- **Account online**:
  - accesso a tutti i sistemi attestati
  - autenticazione tramite account Microsoft

Microsoft Windows
secure boot

- **UEFI**
- **Avvio solo di S.O. Microsoft**
  - *è disabilitabile*

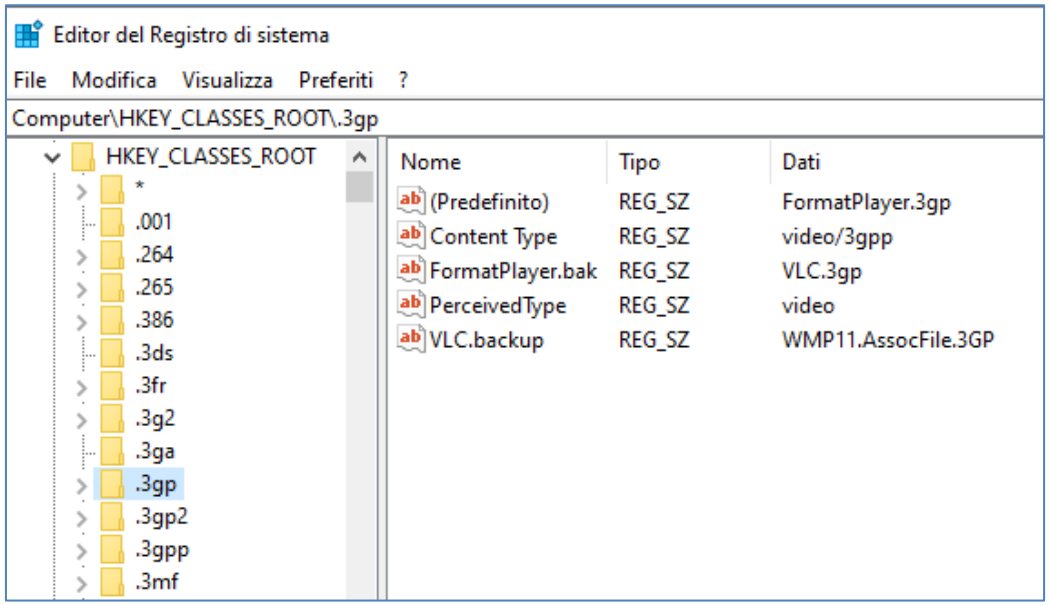


Microsoft Windows
Registro di Sistema

- *Impostazioni del S.O. e di Programmi installati.*
- **Windows 95/98:**
  - User.dat:
    - \Windows
    - \Windows\Profiles*[user_name]*
  - System.dat:
    - \Windows
- **Windows ≥ XP:**
  - Software, System, SAM, Security, Default:
    - \Windows\system32\config
  - NTuser.dat:
    - \Documents and Settings*[user_name] (Windows XP)*
    - \Users*[user_name] (Windows ≥ Vista)*

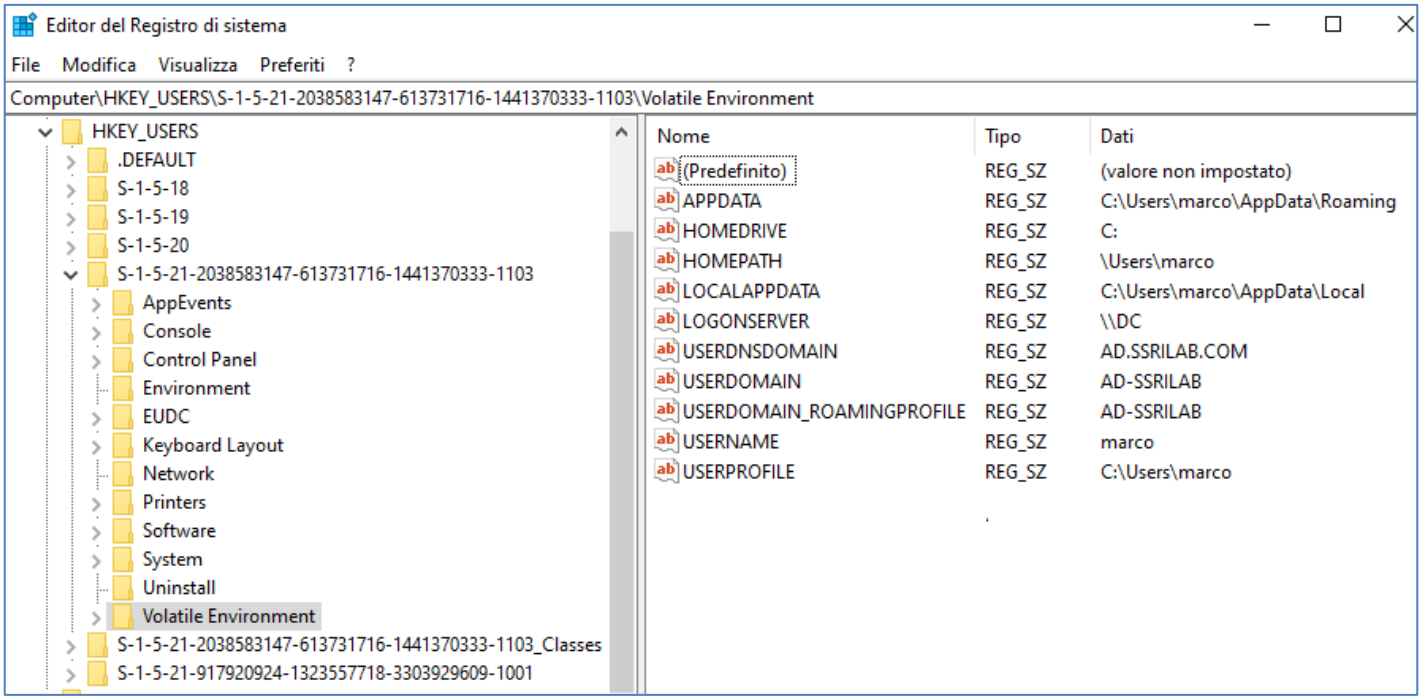
Microsoft Windows
Registro di Sistema

- Struttura ad albero con cinque sotto-alberi principali (**hive**):
  - **HKEY_CLASSES_ROOT:**
    - Associazione: estensione file – applicazione



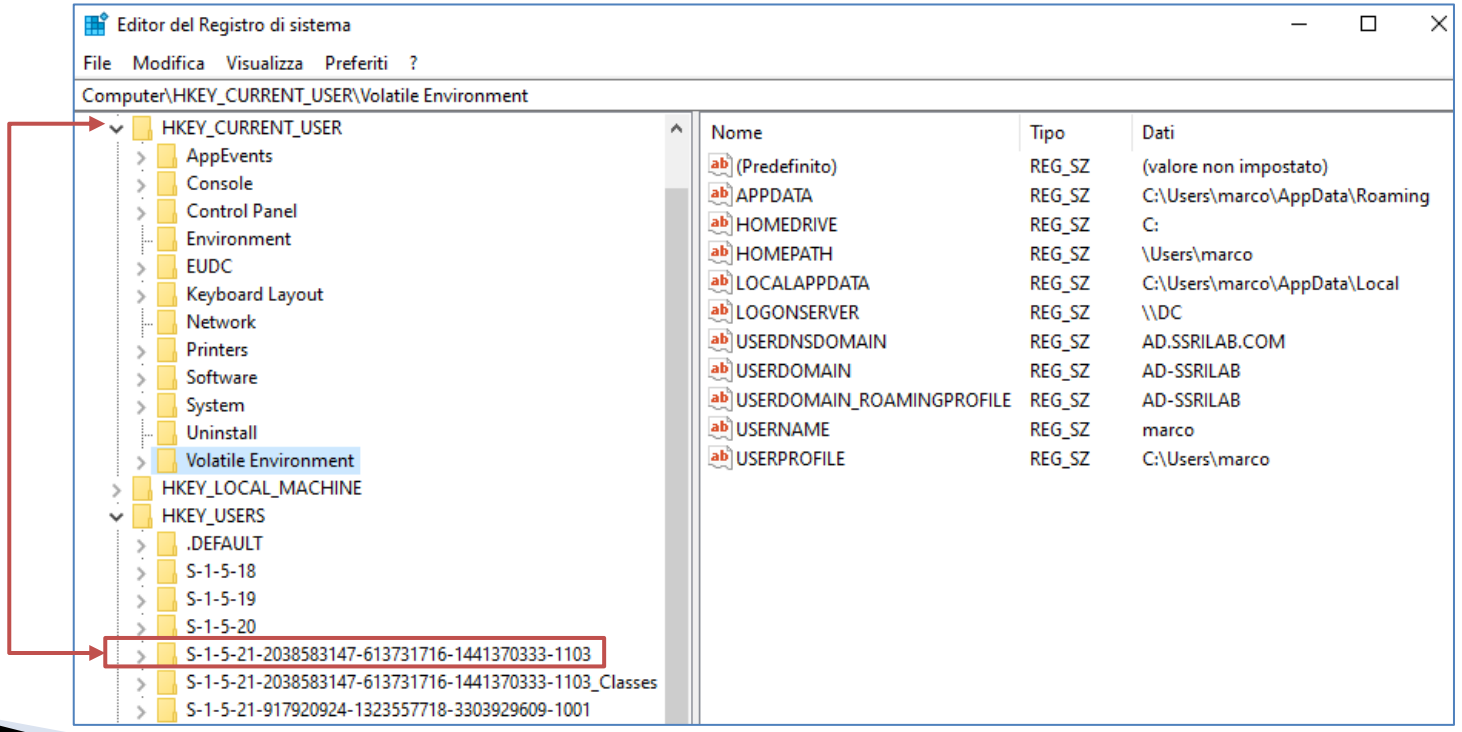
Microsoft Windows
Registro di Sistema

- **HKEY_USERS:**
  - impostazioni di tutti profili utenti configurati nel sistema *(NTuser.dat)*



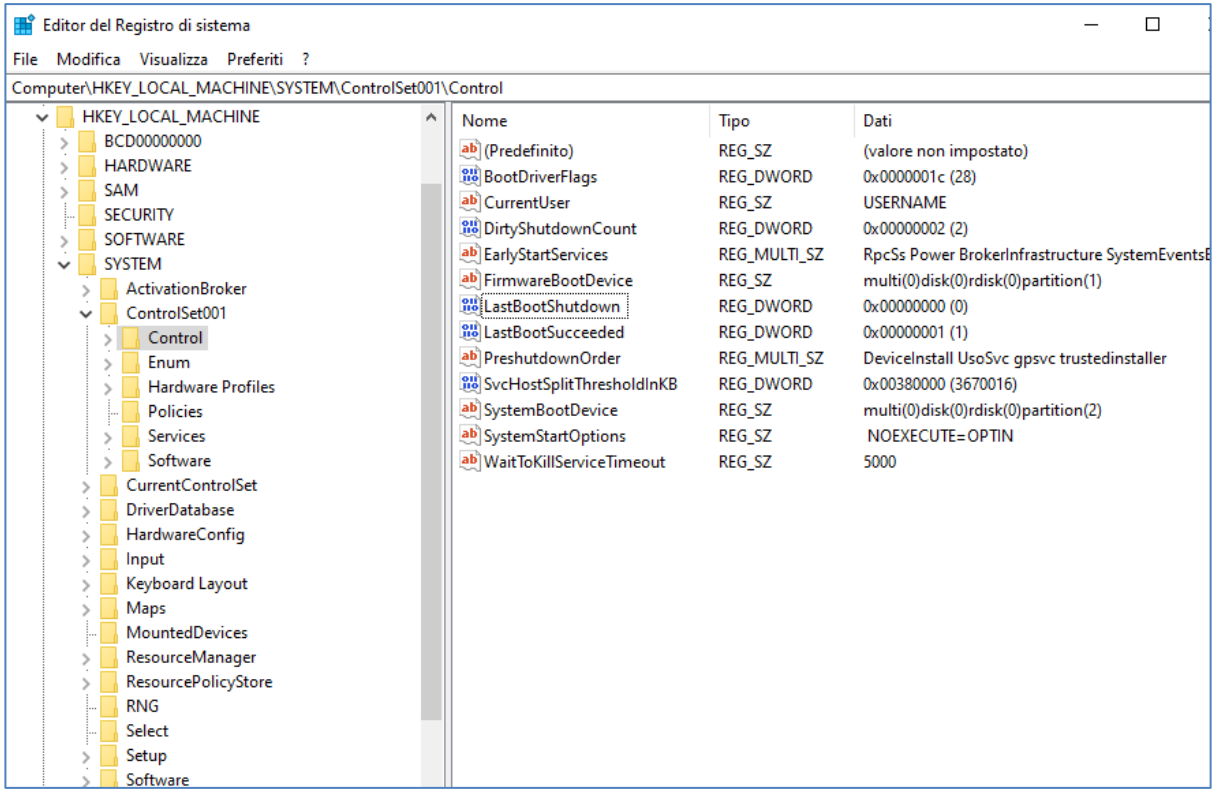
Microsoft Windows
Registro di Sistema

- **HKEY_CURRENT_USER:**
  - puntatore al profilo utente presente in “HKEY_USERS”, loggato nel sistema



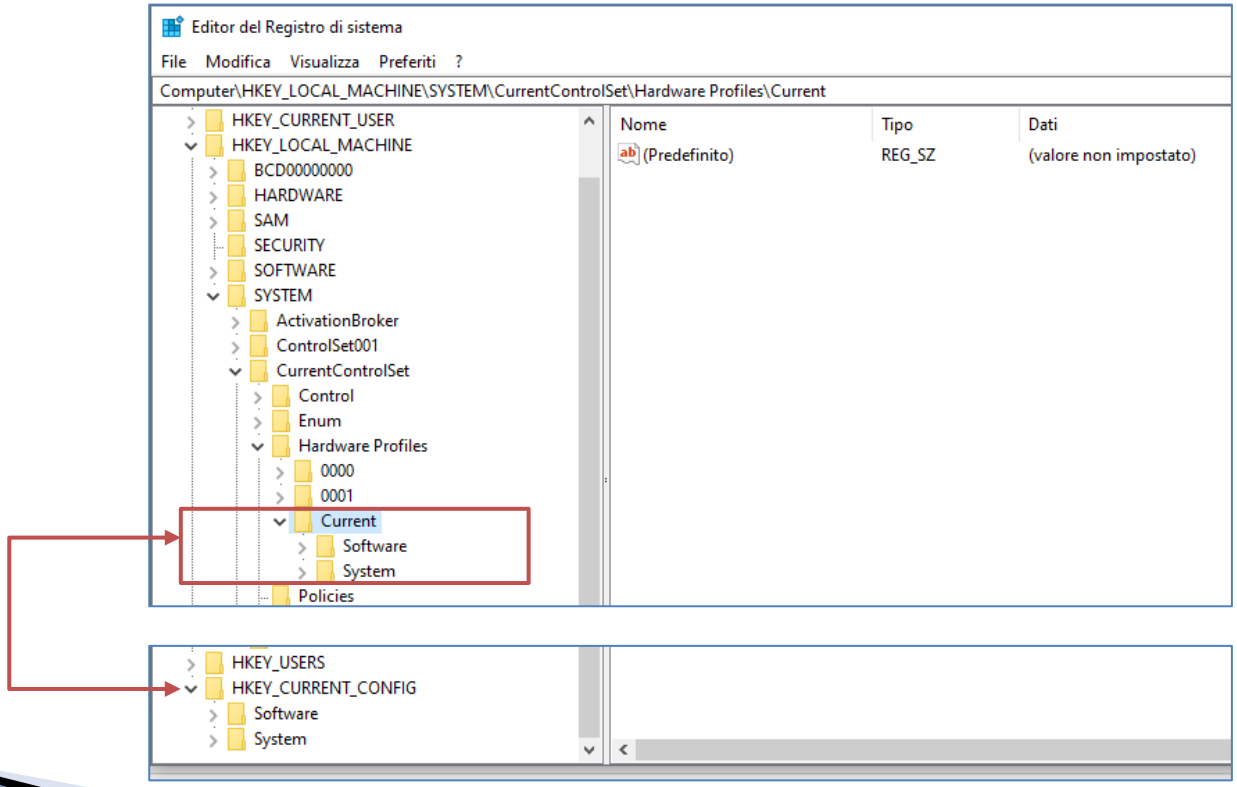
Microsoft Windows
Registro di Sistema

- **HKEY_LOCAL_MACHINE:**
  - configurazione del computer



Microsoft Windows
Registro di Sistema

- **HKEY_CURRENT_CONFIG:**
  - puntatore alla corrente configurazione situata in «HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Hardware Profiles\Current»



Microsoft Windows
Registro di Sistema

- Ogni nodo dell'albero:
  - **Chiave**: coppia di valori (*NomeChiave-Valore*)
  - **Sottochiavi**

Tipi di chiavi	
Tipo	**Descrizione**
REG_SZ	NUL-terminated string
REG_EXPAND_SZ	NUL-terminated string (variabili di ambiente)
REG_BINARY	Dati binari
REG_DWORD/ REG_DWORD_LITTLE_ENDIAN	4Byte (intero senza segno) [little endian]
REG_DWORD_BIG_ENDIAN	4Byte (intero senza segno) [big endian]
REG_LINK	Collegamento ad un'altra chiave
REG_MULTI_SZ	Array di NUL-terminated string

Microsoft Windows
Registro di Sistema

Tipi di chiavi	
Tipo	**Descrizione**
REG_RESOURCE_LIST	Elenco di risorse per un driver
REG_FULL_RESOURCE_DESCRIPTOR	Un descrittore di risorsa utilizzata da un driver
REG_RESOURCE_REQUIREMENTS_LIST	Un elenco requisiti delle risorse di un driver
REG_QWORD / REG_QWORD_LITTLE_ENDIAN	8Byte (intero senza segno) [little endian]
REG_NONE	Nessun tipo

Microsoft Windows
Registro di Sistema: Analisi

- Configurazioni dell'utente
- Dispositivi USB: *pendrive, dischi esterni, etc.*
- Informazioni temporali: data di ultima modifica delle chiavi
- Strumenti:
  - RegEdit *(Windows)*
  - Windows Registry Recovery *(Mitec)*
  - Registry Viewer *(Access Data)*

Microsoft Windows
Thumbnails

- *miniature delle immagini presenti nelle cartelle*

Microsoft Windows
Thumbnails

- **Windows 98 – XP:**
  - Thumbs.db:
    - In ogni cartella in cui sono\erano presenti immagini
- **Windows ≥ Vista:**
  - Database centralizzato thumbcache_*[NUM]*.db

    [NUM]: dimensioni delle anteprime: 96, 256, 1024
    - %userprofile%\AppData\Local\Microsoft\Windows\Explorer

- **ANALISI**: miniature di immagini non più presenti
  - Thumbs Viewer
  - Thumbcache Viewer

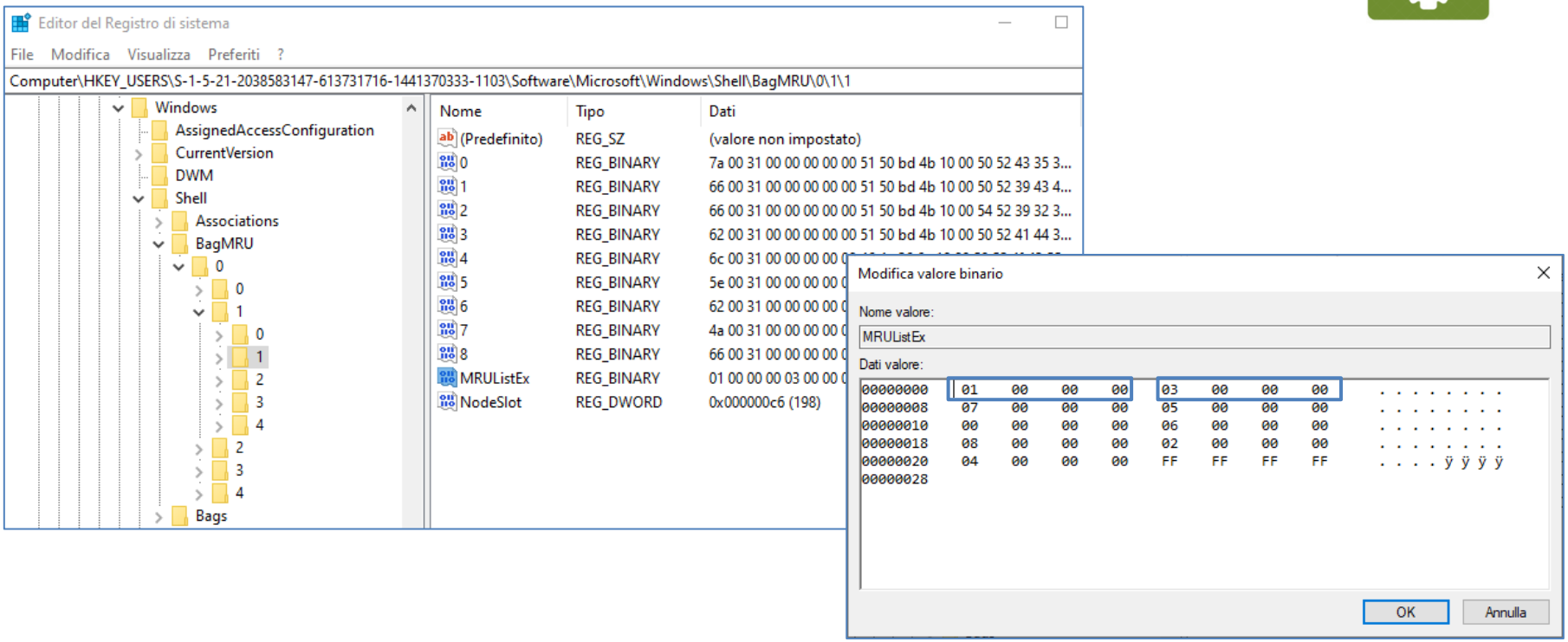
Microsoft Windows
ShellBag

- *Personalizzazioni utente delle visualizzazione del contenuto delle cartelle*

- **Chiavi di registro**
  - HKEY_USERS\ <*USERID*>\Software\Microsoft\Windows\ Shell\
  - HKEY_USERS \ <*USERID*>\Software\Microsoft\Windows\ ShellNoRoam ***(Windows < Vista)***
  - HKEY_USERS \ <*USERID*>\ Software\Classes\LocalSettings \Software\Microsoft\Windows\Shell\ ***(Windows ≥ Vista)***

Microsoft Windows

ShellBag

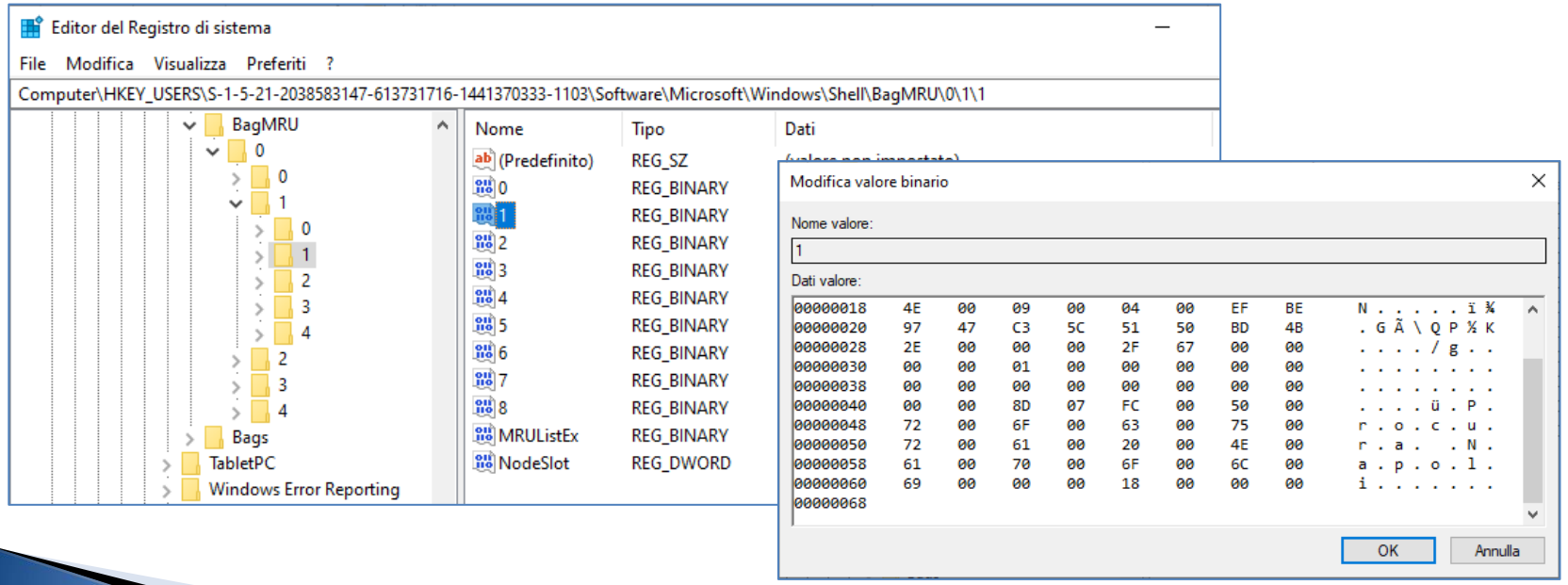


- **BagMRU**: storico di tutte le cartelle visualizzate dall'utente
- **Bags**: impostazioni di visualizzazione delle cartelle contenute in BagMRU

Microsoft Windows

ShellBag: analisi

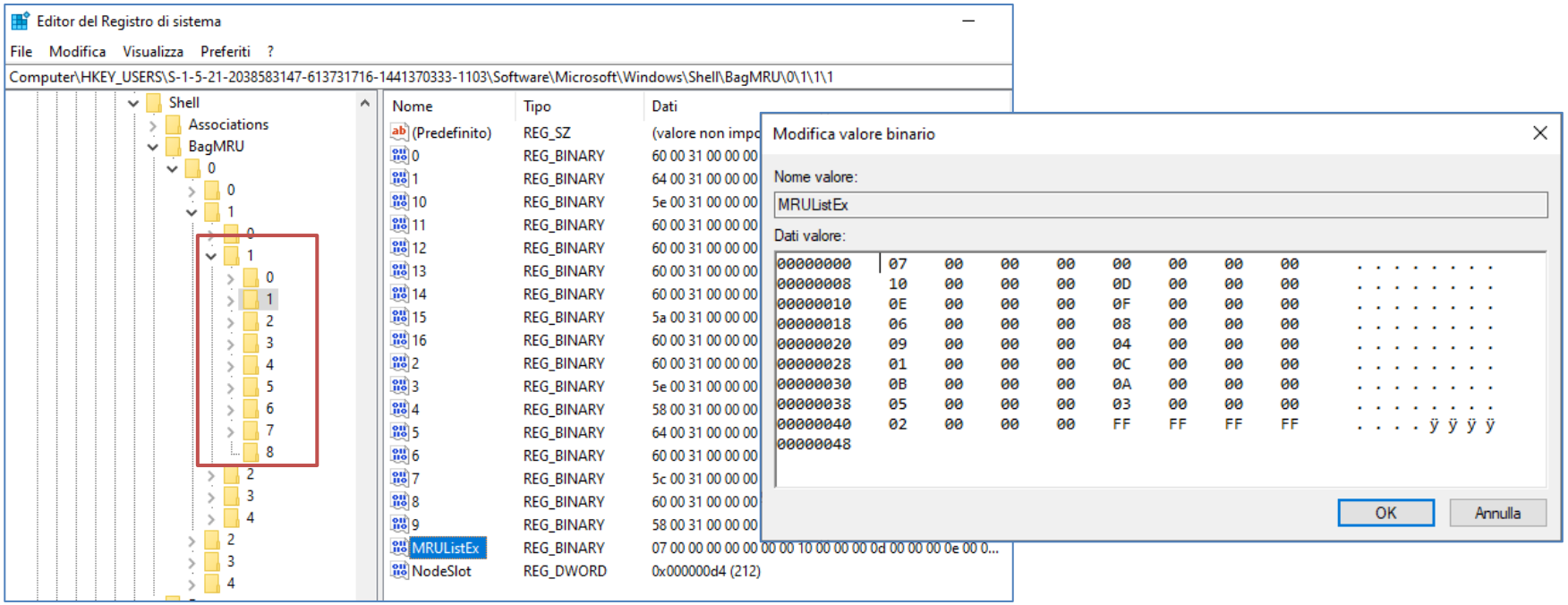
1) Si segue la lista delle cartelle presenti in MRUListex *(Es.: 1)*
   - Si seleziona visualizza il valore della chiave relativa: nome cartella *(Es.: Procura Napoli)*



Microsoft Windows

ShellBag: analisi

2) Si segue la sottochiave della cartella (*Es.: 1*)
   - Si visualizza la chiave MRUListex e si continua ricorsivamente la sua esplorazione



Microsoft Windows

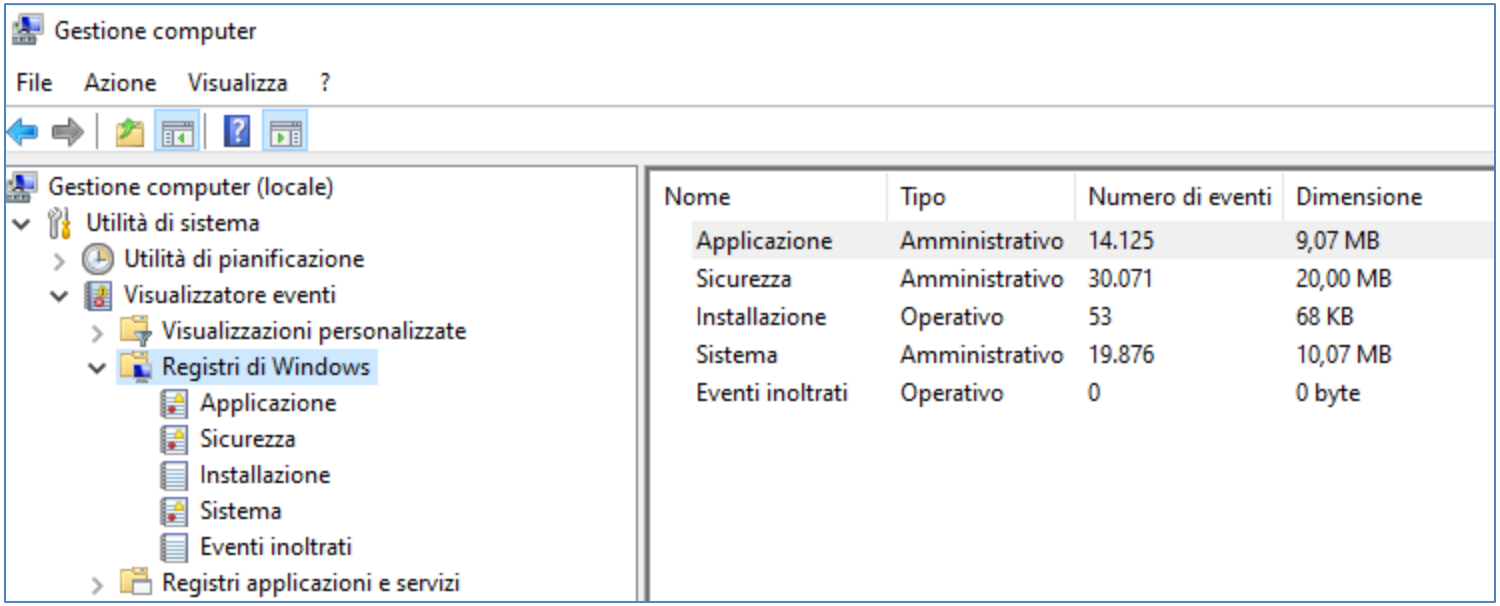
ShellBag: analisi

- Informazioni ottenibili:
  - **Bag Number**: la sottochiave Bags che contiene le preferenze dell'utente (Nodeslot).
  - **Registry key last write time**: data di primo accesso o di ultima modifica della cartella.
  - **Folder name**: nome della cartella.

- **Tool**: ShellBagsView *(NirSoft)*

Microsoft Windows
Event Viewer

- Sistema di *logging* standard (EVT/EVTX)



Microsoft Windows

Event Viewer

ID Evento ≥ Vista	ID Evento < Vista	Descrizione
1102	517	Log di audit cancellato
4624	528/540	Accesso di un account completato
4625	529/537	Accesso non riuscito per un account
4634	538	Un account è stato disconnesso
4674	578	Operazione eseguita con privilegi elevati
4704	608	Assegnazione di un diritto per un utente
4719	612	Cambiamento nelle politiche di audit
4720	624	Aggiunta di un nuovo account
4722	626	Un account utente è stato abilitato
4726	630	Un account utente è stato eliminato
4732	636	Un account utente è stato aggiunto ad un gruppo locale
4738	642	Un account utente è stato modificato
4739	643	Cambiamento nelle policy di dominio.

Microsoft Windows
Application Data

- *impostazioni dei programmi utilizzati dall'utente e file temporanei*

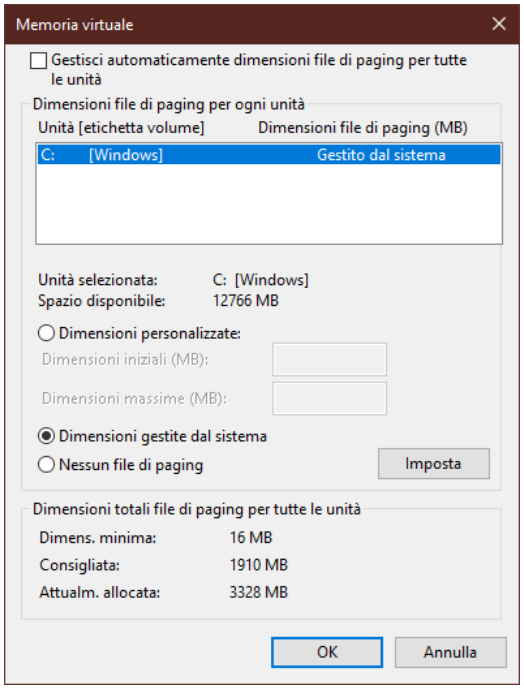
- **Windows XP**:
  - \Documents and Settings\[nome_utente]\
    - **Dati Applicazioni**
    - **Impostazioni Locali**
- **Windows ≥ Vista:**
  - \Users\[nome_utente]**AppData**

Microsoft Windows
Application Data: Analisi

- quadro complessivo dell'utilizzo del computer da parte di un utente:
  - **Posta elettronica**
  - **Cache**
  - **Cronologia**
  - **Log**
  - **Configurazioni**

Microsoft Windows
File Swap

- *Estensione della memoria volatile (RAM)*
  - **Pagefile.sys**



- **Hiberfil.sys**: congelamento della memoria RAM in fase di sospensione\ibernazione

Microsoft Windows
Analisi

Vantaggi

- Diffuso
- Documentato
- Supportato

Svantaggi

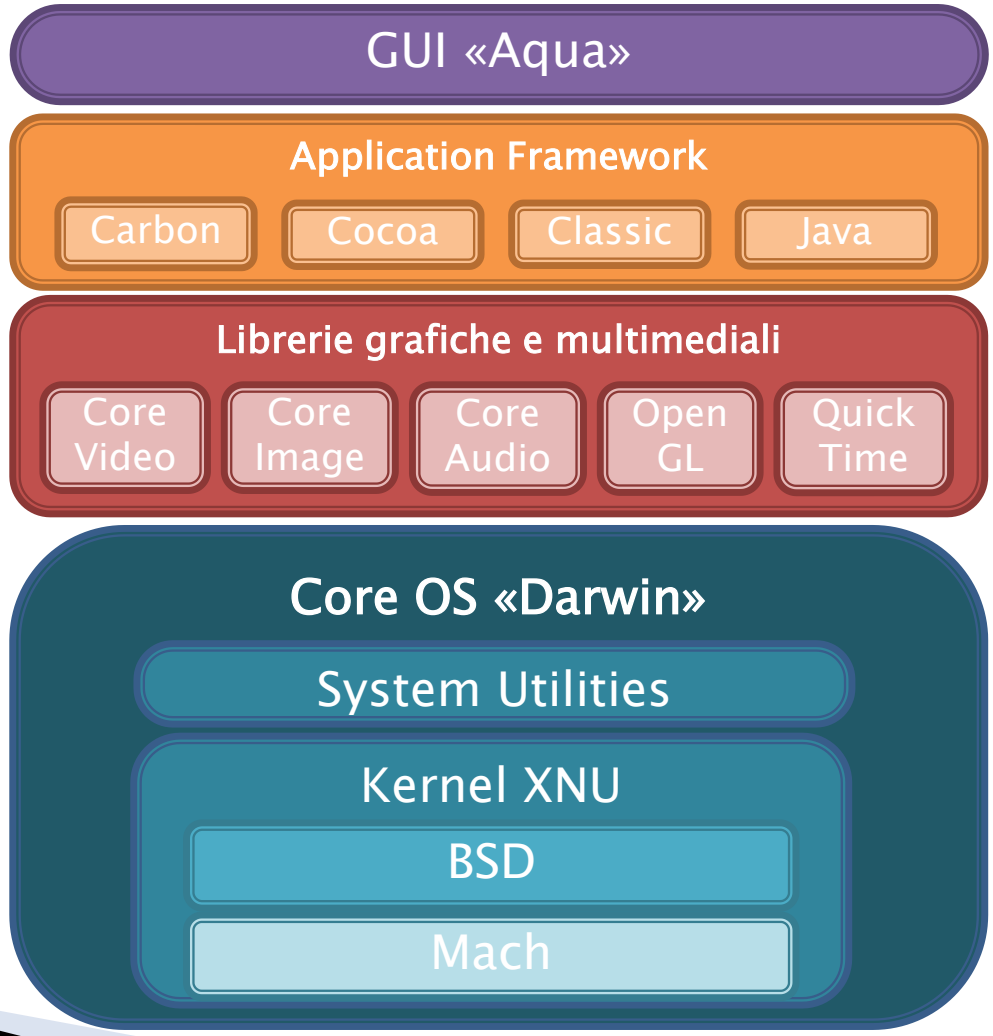
- Pochi log
- Presenza di antivirus che possono compromettere una timeline
- Sistema commerciale

Sistemi Operativi

- Apple OS X/macOS

Apple OS X/macOS

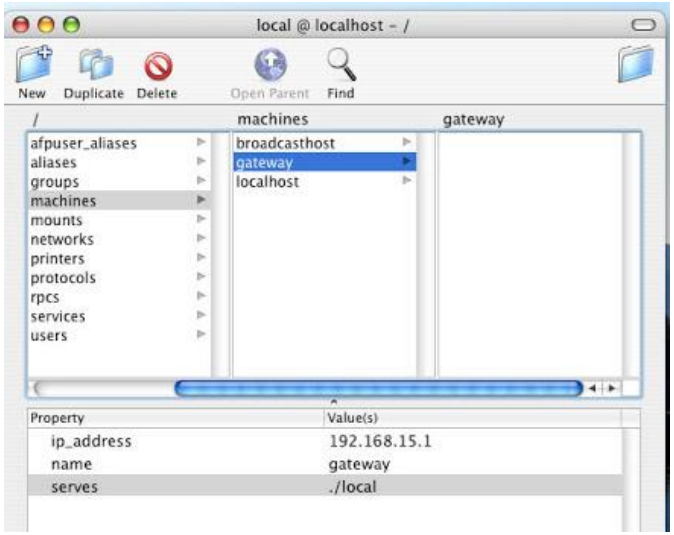
overview



Apple OS X/macOS
configurazione

- NetInfo (DB ad oggetti)
  - Controlla diverse configurazioni del S.O.
    - Entry statiche di rete (file hosts)
    - Definizione di tutti gli utenti
- Gestione NetInfo:
  - /Application/Utility (OS X ≤ 10.4)
  - /Application/Utility/Utility Directory (OS X >10.4)

Fino alla versione Mac OS X 10.5



Apple OS X/macOS
configurazione server

- Open Directory (Mac OS X Server 10.4)
  - Servizio di directory
  - Gestione delle autenticazioni

Tool	Descrizione
dscl	Manipolazione e gestione dei servizi di directory
dsconfigldap	manipolazione degli alberi LDAP
dsconfigad	manipolazione dei sistemi Active Directory
dseditgroup	gestione di gruppi di utenti
dsenableroot	abilita/disabilita l'utente root in OpenDirectory
dscacheutil	regola le cache relative a OpenDirectory
dsmemberutil	Gestisce i gruppi di appartenenza di un oggetto OpenDirectory
dsexport	esporta oggetti da un albero OpenDirectory
dsimport	importa oggetti in un albero OpenDirectory

Apple OS X/macOS
cifratura

- **FileVault**
  - Cifratura della home directory (/Users/[nome_utente]
- **FileVault 2** *(OS X ≥ 10.7)*
  - Full disk encryption

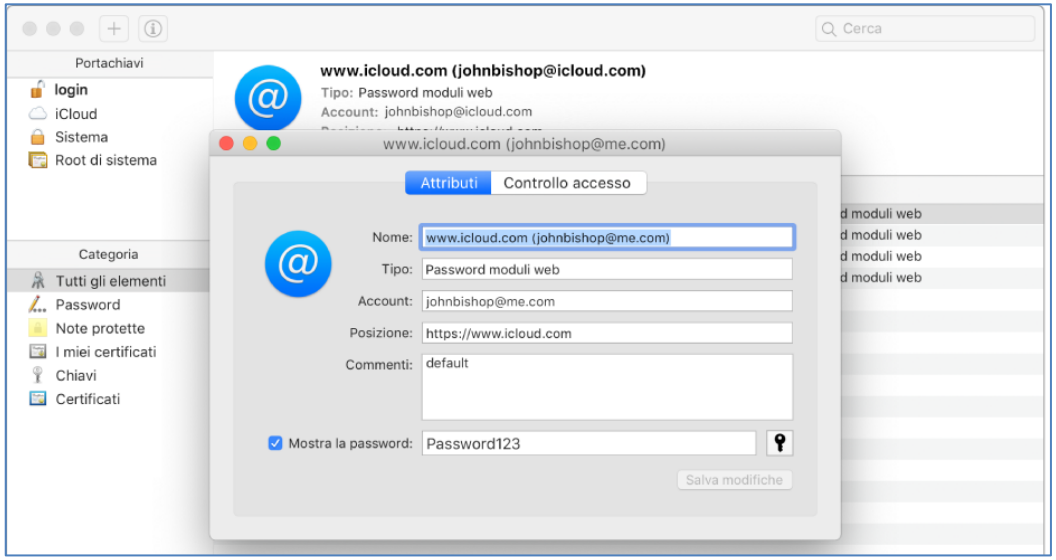
Apple OS X/macOS
file swap

- Estensione della memoria volatile (RAM)
  - */private/var/vm/**swapfile****
- congelamento della memoria RAM in fase di sospensione:
  - */private/var/vm/**sleepimage***

Apple OS X/macOS
portachiavi

- Accentramento delle credenziali utente
  - Accesso tramite API
  - Cifratura AES-128

- OS X ≥ 10.9
  - Integrazione servizio Apple iCloud



Apple OS X/macOS
analisi

- Elevato numero di tecnologie proprietarie
  - Uso di un sistema OS X per l'analisi

- Strumenti:
  - *BlackBag Technologies*
    - **Blacklight**: toolkit forense
    - **MacQuisition**: tool di acquisizione forense
  - Mac Forensics Lab *(SubRosaSoft)*

  - **Apple hdiutil**: *tool da riga di comando*
    - Apple DMG
      - Copia FullDisk
      - Copia Logica

Apple OS X/macOS
analisi

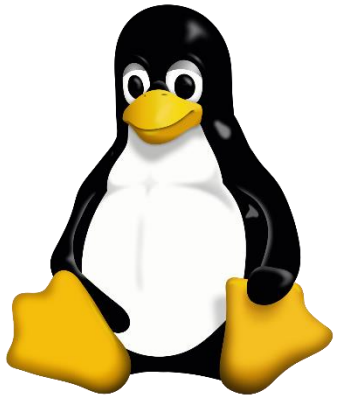
- **Home Directory Utente**
  - La granparte dei file dell'utente
  - Dati delle applicazioni: */Users/[nome_utente]/Library*

Sistemi Operativi

- Linux

Linux
overview

- **Distribuzioni basate su kernel GNU/Linux**
- **Linux Standard Base (LSB)**
  - Standardizzazione delle diverse distribuzioni
- **Componenti:**
  - Kernel
  - Librerie di sistema
  - Tool di base



Linux
overview





- **Distribuzioni commerciali:**
  - Red Hat Enterprise
    - Fedora
    - CentOS: versione libera senza supporto
    - Scientific Linux
  - SUSE Linux Enterprise
    - openSUSE

- **Distribuzioni gratuite:**
  - Debian: distribuzione ufficiale della Free Software Foundation
  - Ubuntu


Linux
sistema

- **Multiutente e Multitasking**
- **Struttura rigida del file system:**

Directory	Contenuto
/bin	Binari d'uso comune nel sistema.
/boot	Kernel e file necessari al boot
/dev	device fisici e logici collegati al computer
/etc	File di configurazione del sistema
/home	File degli utenti
/lib	Librerie di sistema
/mnt	Punto di montaggio per media esterni
/opt	Punto dove sono installati programmi che richiedono complesse alberature per il loro funzionamento
/root	Home directory dell'utente root

Linux
sistema

Directory	Contenuto
/sbin	Binari riservati all'uso di root
/srv	File di dati per alcuni servizi server come web e server FTP
/tmp	Locazione generale per i file temporanei
/usr	Contiene programmi non indispensabili al sistema
/usr/local	Locazione per i programmi compilati dagli utenti
/usr/src	Sorgenti dl kernel e dei vari pacchetti
/var	Parte variabile dei programmi. Contiene log, mail, spool di stampa, database e quanto può essere utile a un programma da tenere in una directory scrivibile

Linux
sistema

Device /dev	Contenuto
/hda	Disco ATA master collegato al canale primario
/hdd	Disco ATA slave collegato al canale secondario
/sda	Disco SCSI con l'ID più basso collegato alla catena
/hda1	Prima partizione del disco ATA master collegato al canale primario
/loop0	Loop device. Permette visualizzare un file immagine come se fosse realmente agganciato
/eth0	Prima scheda di rete collegata al sistema
/md0	RAID software generato da Linux

Linux
sistema

- **Sistema di permessi di file e directory:**
  - **r**: permesso di lettura
  - **w**: permesso di scrittura
  - **x**: ***file*** permesso di esecuzione | ***directory*** permesso di accesso

r	w	x	r	w	x	r	w	x
owner			group			public		

  - **Utente root**: *nessun limite*

Linux
Log

- **Syslog**: sistema di gestione Log
  - **syslogd**: daemon *(servizio)*
  - *configurazione*: /etc/**syslog.conf**

Facility code	Keyword	Description
0	kern	Kernel messages
1	user	User-level messages
2	mail	Mail system
3	daemon	System daemons
4	auth	Security/authentication messages
5	syslog	Messages generated internally by syslogd
6	lpr	Line printer subsystem
7	news	Network news subsystem
8	uucp	UUCP subsystem
9	cron	Clock daemon

Linux
Log

Facility code	Keyword	Description
10	authpriv	Security/authentication messages
11	ftp	FTP daemon
12	ntp	NTP subsystem
13	security	Log audit
14	console	Log alert
15	solaris-cron	Scheduling daemon
16-23	local0 – local7	Locally used facilities

Severity Value	Severity	Description
0	Emergency	System is unusable
1	Alert	Action must be taken immediately
2	Critical	Critical conditions
3	Error	Error conditions
4	Warning	Warning conditions
5	Notice	Normal but significant conditions
6	Informational	Informational messages
7	Debug	Debug-level messages

Linux
Log

- Posizione dei log: */var/log*
  - **messages:** eventi relativi alla macchina
  - **wtmp**: registrazione degli accessi

- **Logfinder**: ricerca di tutti i file log

Linux
configurazioni

- posizione:
  - /etc *(configurazione di default)*
    - Inittab: file di configurazione di boot
    - passwd: elenco degli utenti
    - shadow: password degli utenti
  - File nascosti nella home directory utente *(configurazioni personalizzate)*
- Nome_programma.conf *(Es.:apache.conf)*

swap

- *Partizione:*
  - *FAT*
  - *0x83 (marcatore)*

Linux
home directory

- Tipi di utente:
  - **root**: amministratore di sistema *(sys-admin)*
  - **utente comune**

- Directory disponibili all'utente:
  - /usr/local/bin: file dei programmi utilizzabili dall'utente
  - /tmp: file temporanei
  - /home/*[nome_utente]:* directory principale dell'utente
    - ***Dati dell'utente:*** la gran parte dei file creati\gestiti dall'utente
    - ***Shell history:*** lista dei comandi impiegati dall'utente
    - ***Cache***
    - ***File di configurazione:*** configurazioni personalizzate di programmi

Linux
/var

- Contiene di dati cambiano/variano durante la normale esecuzione del sistema
  - Specifico per ogni sistema
- **Dati**:
  - log di sistema;
  - spool di stampa;
  - mail in transito e code;
  - tablespace degli RDBM;
  - cache di sistema;
  - configurazione dei vari tool;
  - database dei pacchetti installati;
  - file di bind;
  - database di LDAP;
  - database di sistema di AFS;
  - database di Kerberos.

Linux
analisi

- /home
- /etc
- /var

- Analisi live:

  1) **inittab/systemd**: controllare tutti i servizi (deamon) eseguiti in fase di boot

  2) **Autenticazione**: verificare la configurazione PAM, kerberos e openLDAP

  3) **\etc\fstab**: verificare il montaggio dei file system all'avvio

SSRI Lorenzo Laurato s.r.l.

Via Coroglio nr. 57/D (BIC- Città della Scienza)
80124 Napoli

Tel. 081.19804755
Fax 081.19576037

lorenzo.laurato@unina.it
lorenzo.laurato@ssrilab.com

www.docenti.unina.it/lorenzo.laurato
www.computerforensicsunina.forumcommunity.net