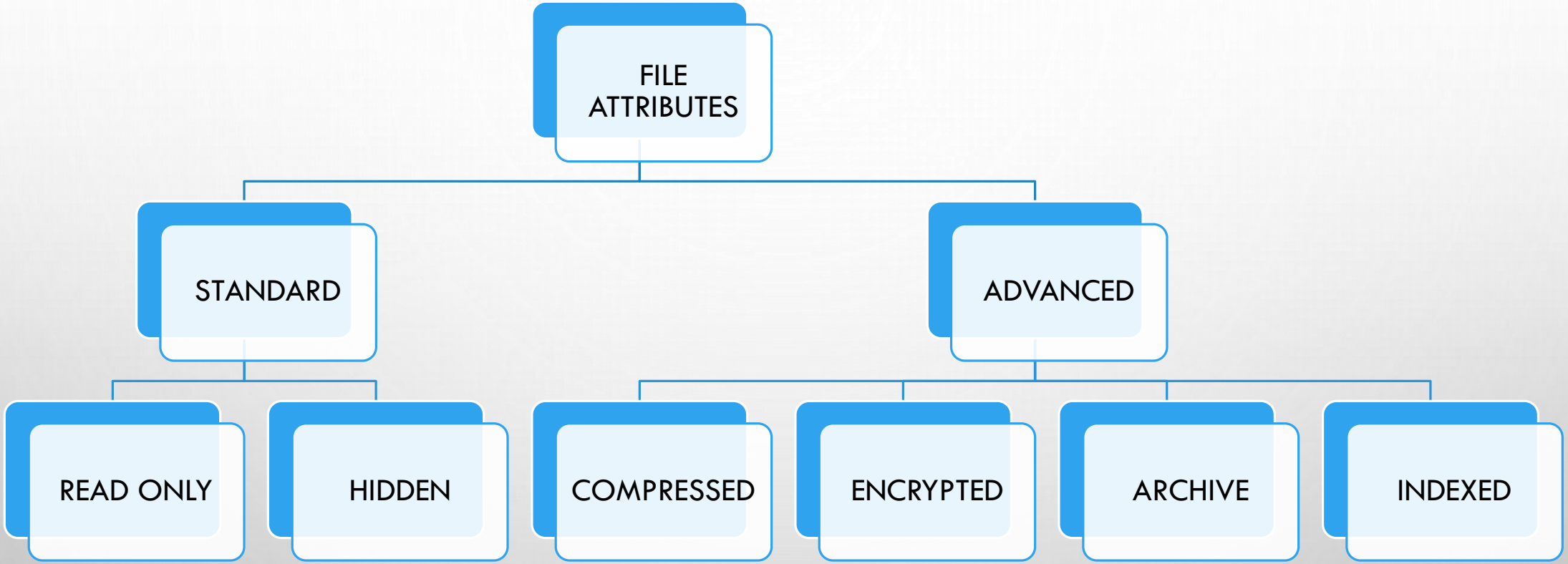
MODERN OPERATING SYSTEMS

LECTURE 7

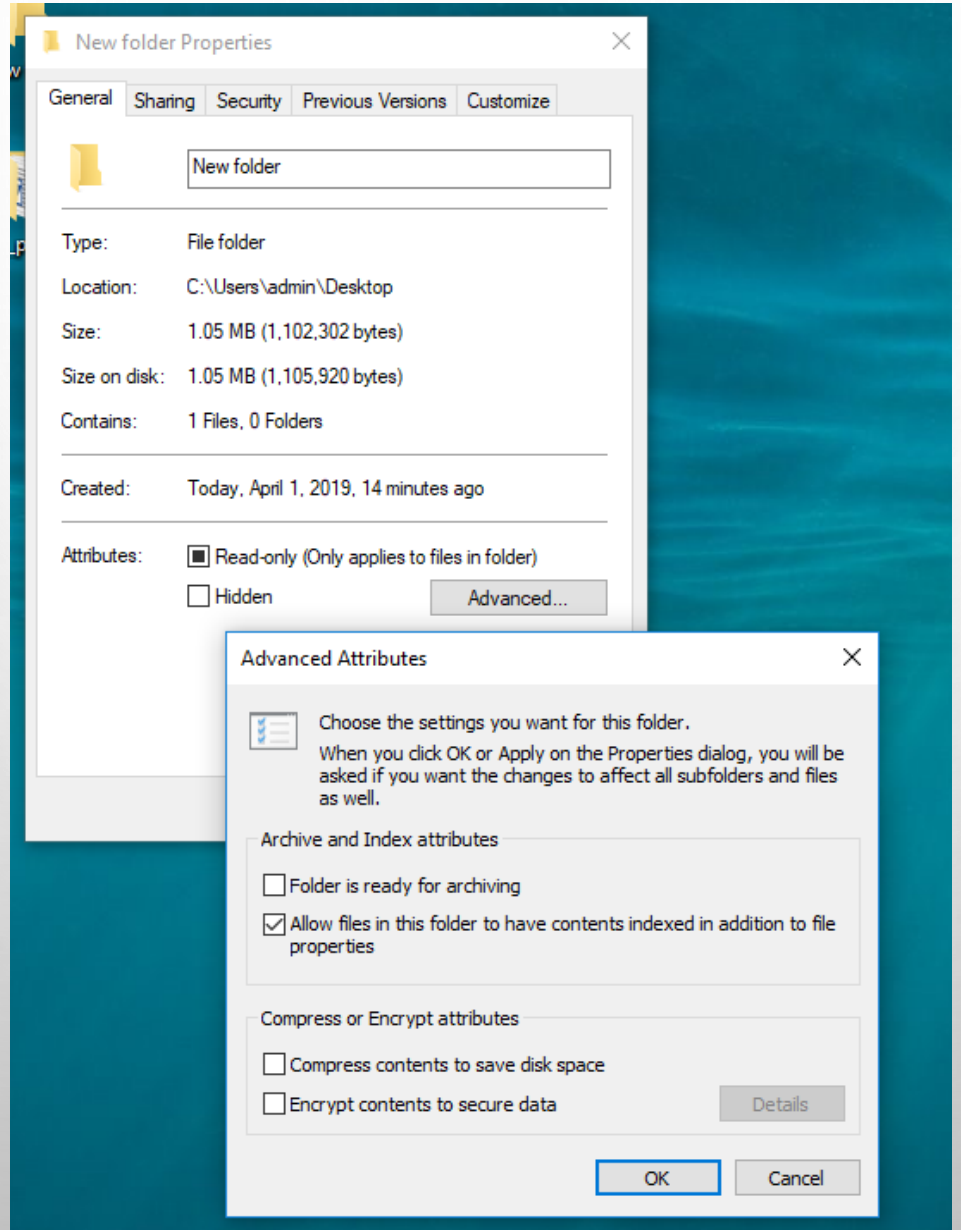
AUTHOR: DR. ZVEREVA OLGA M.

AGENDA

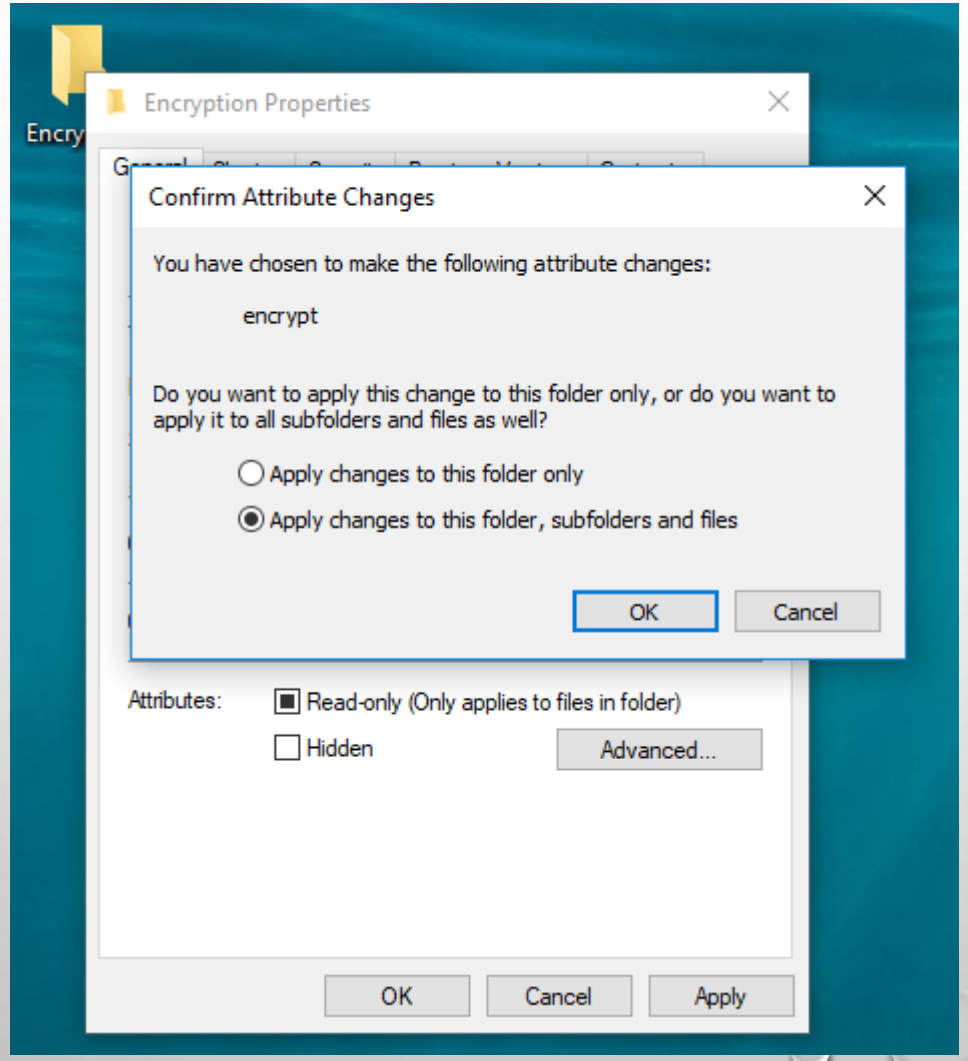
- ✓ NTFS OPERATING PECULIARITIES
- ✓ REGISTRY AS THE “HEART” OF WINDOWS


FILE ATTRIBUTES
STANDARD
ADVANCED
READ ONLY
HIDDEN
COMPRESSED
ENCRYPTED
ARCHIVE
INDEXED

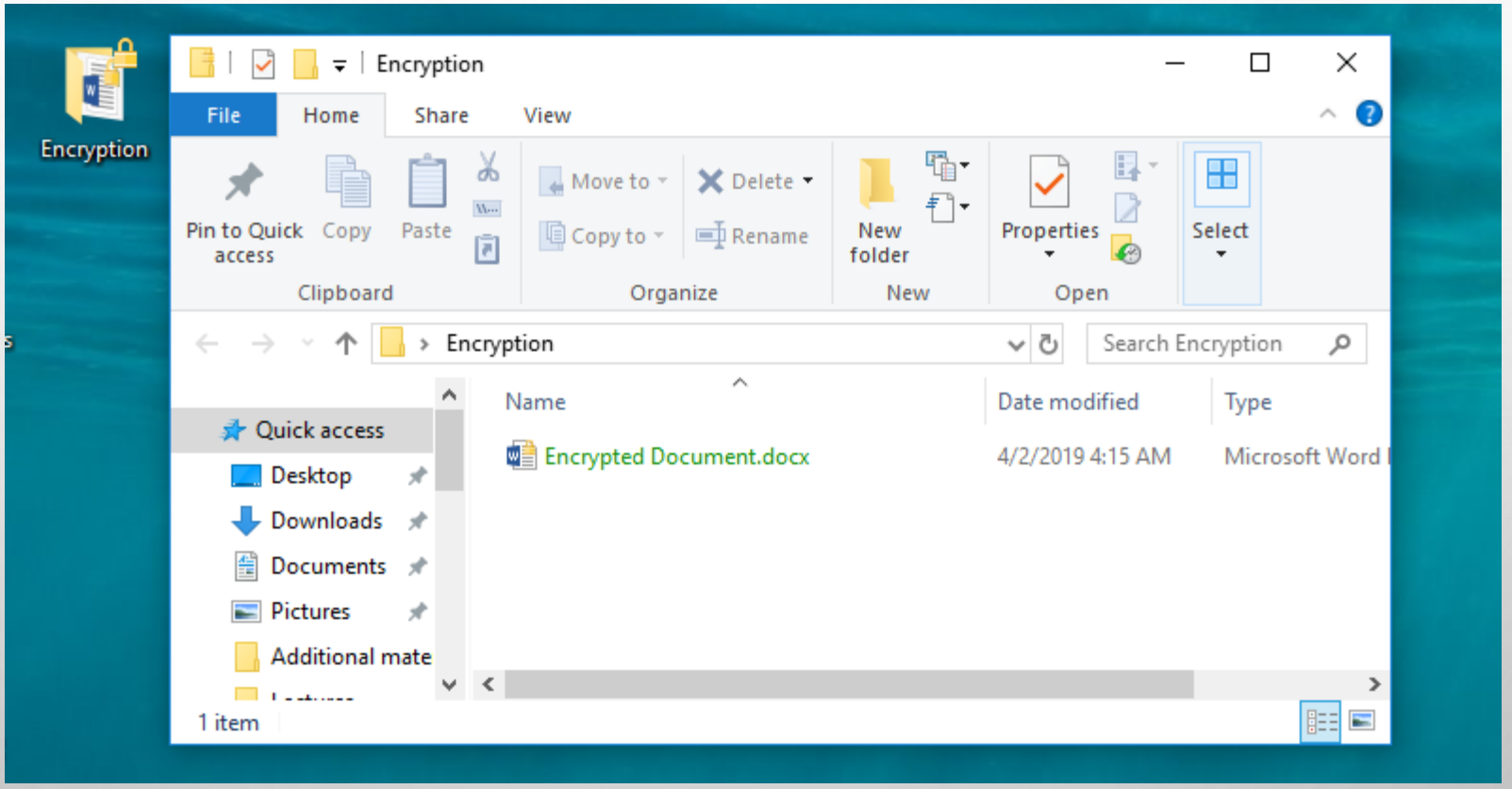
FILE ATTRIBUTES



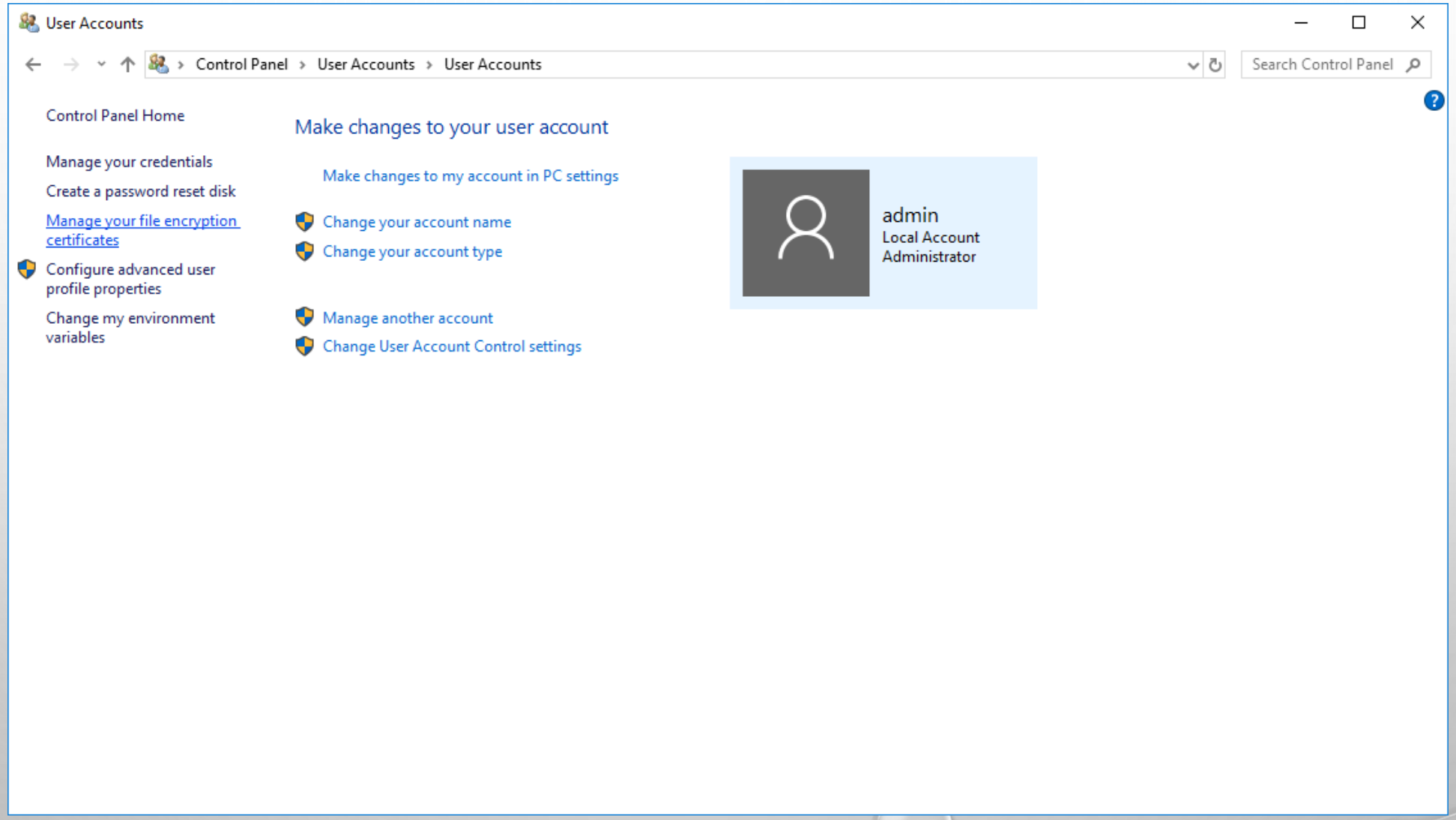
ENCRYPTING FOLDER & FILES



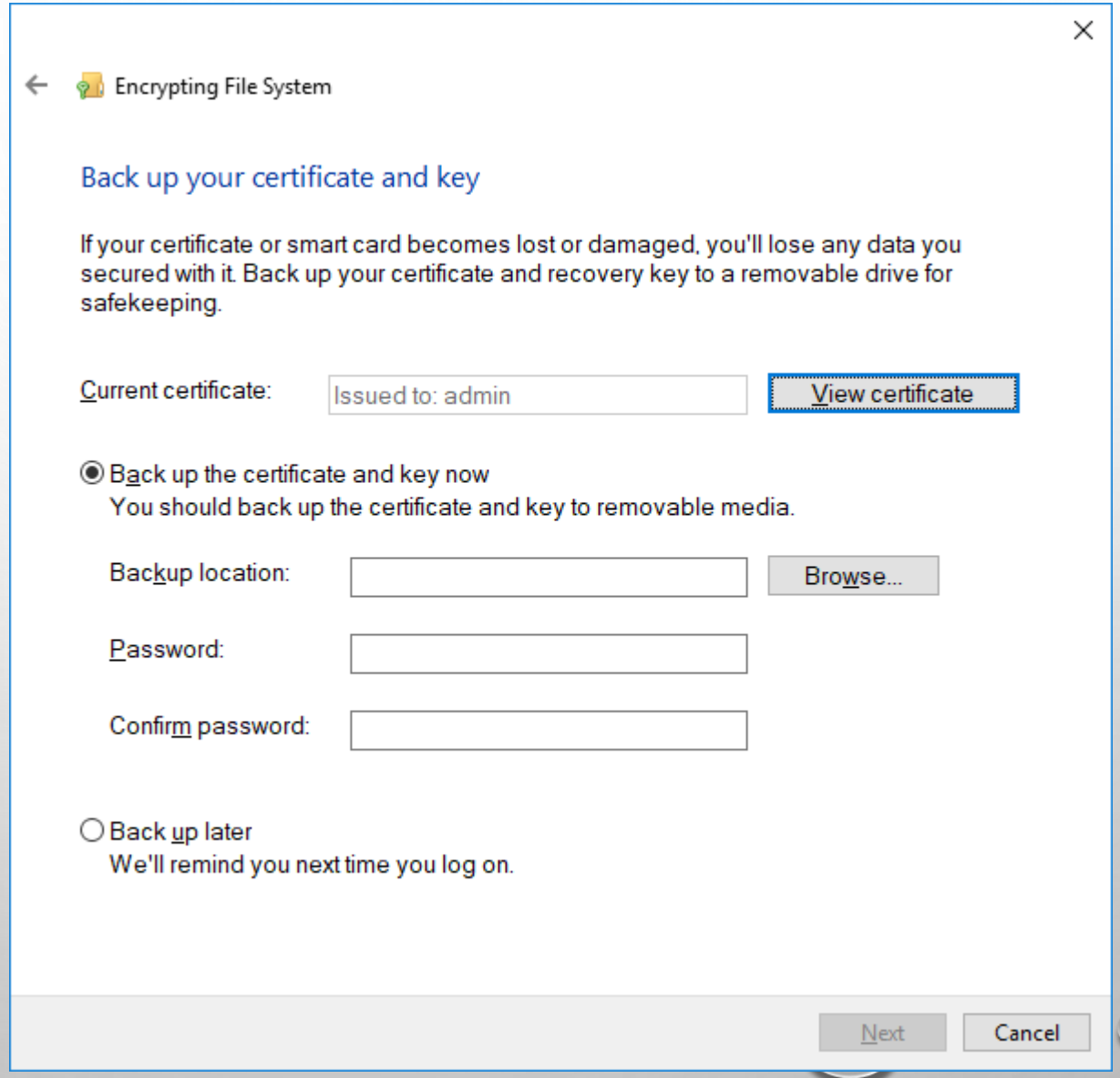
ENCRYPTED FOLDER AND FILE



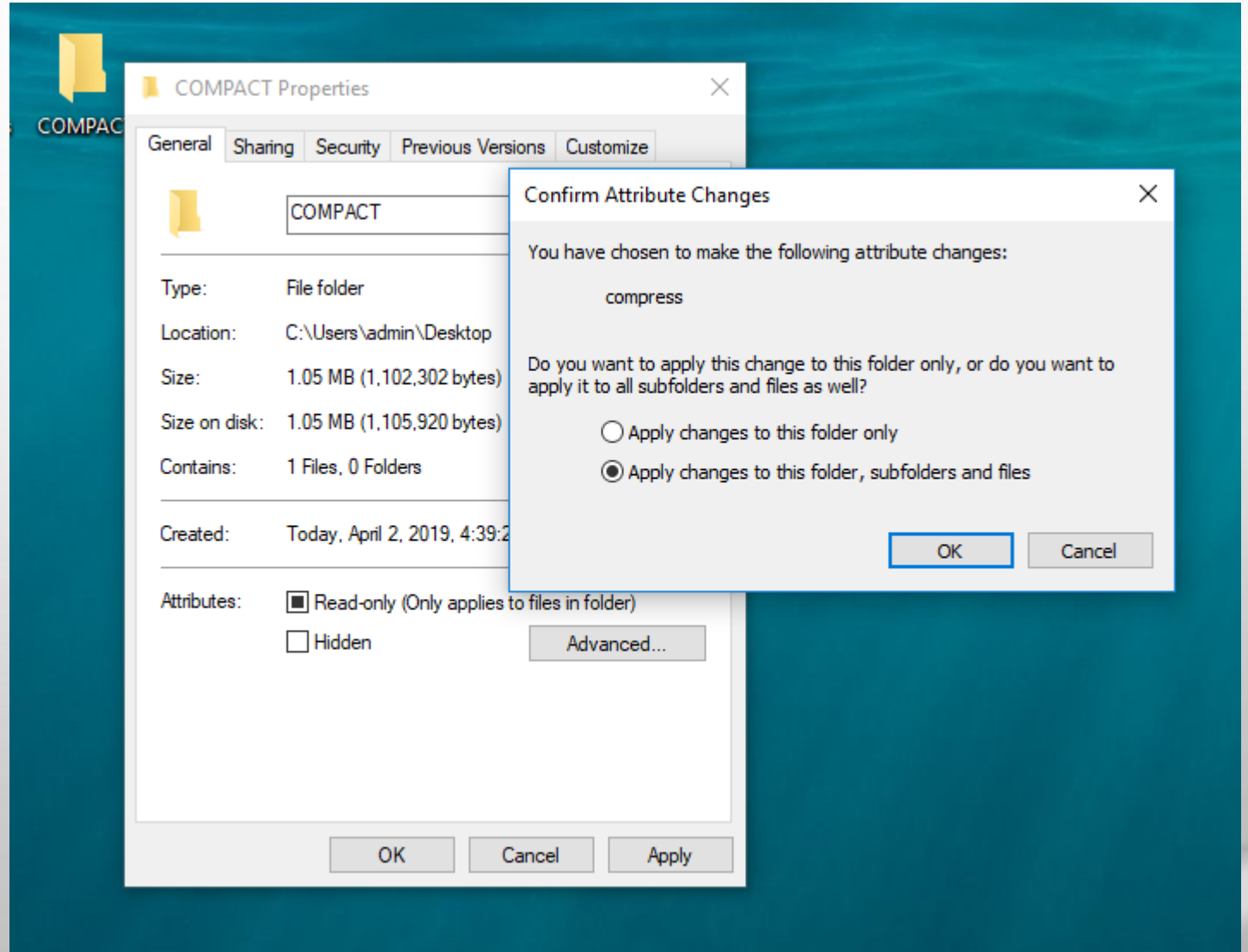
CERTIFICATE MANAGEMENT



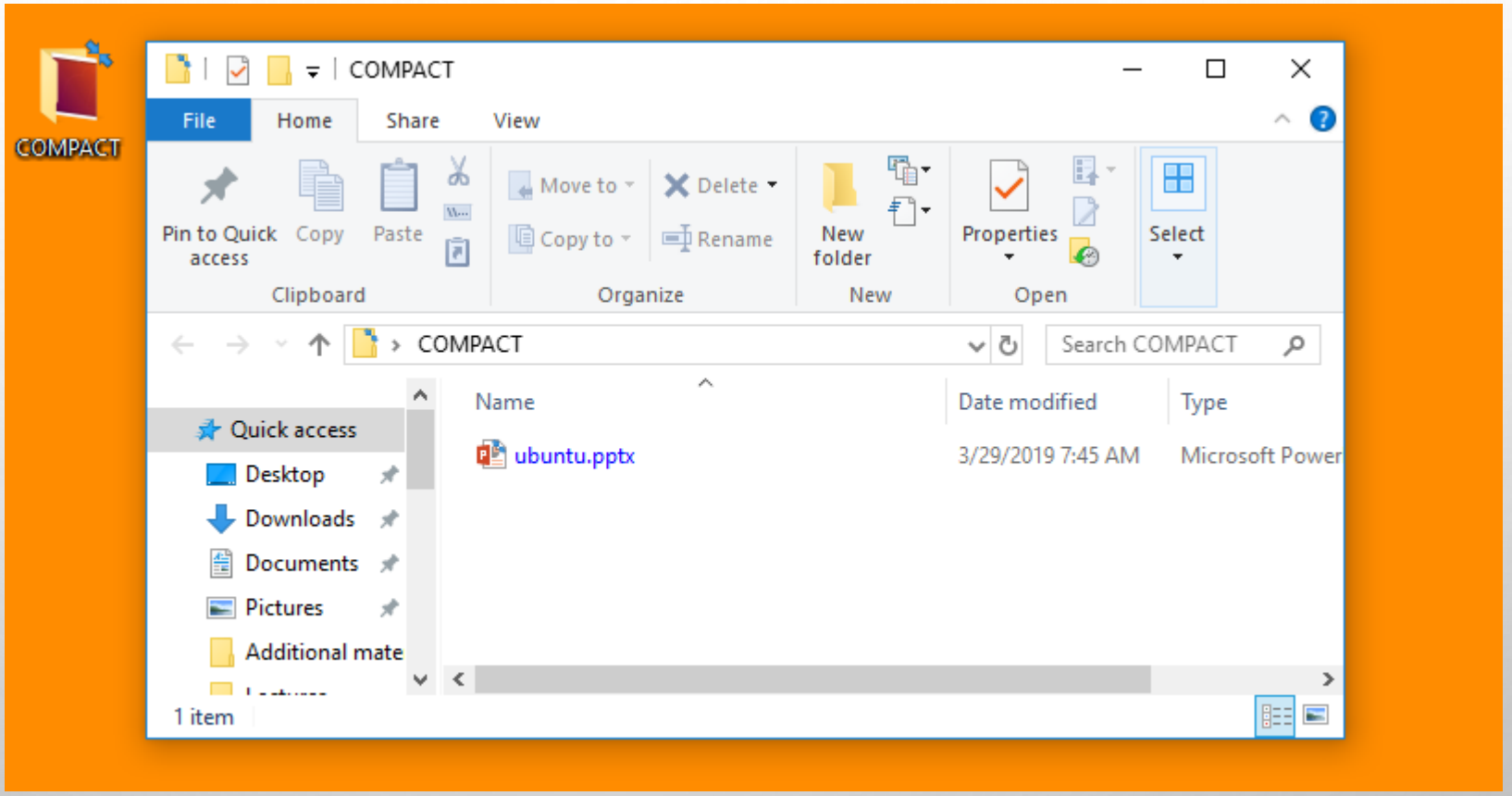
CERTIFICATE MANAGEMENT



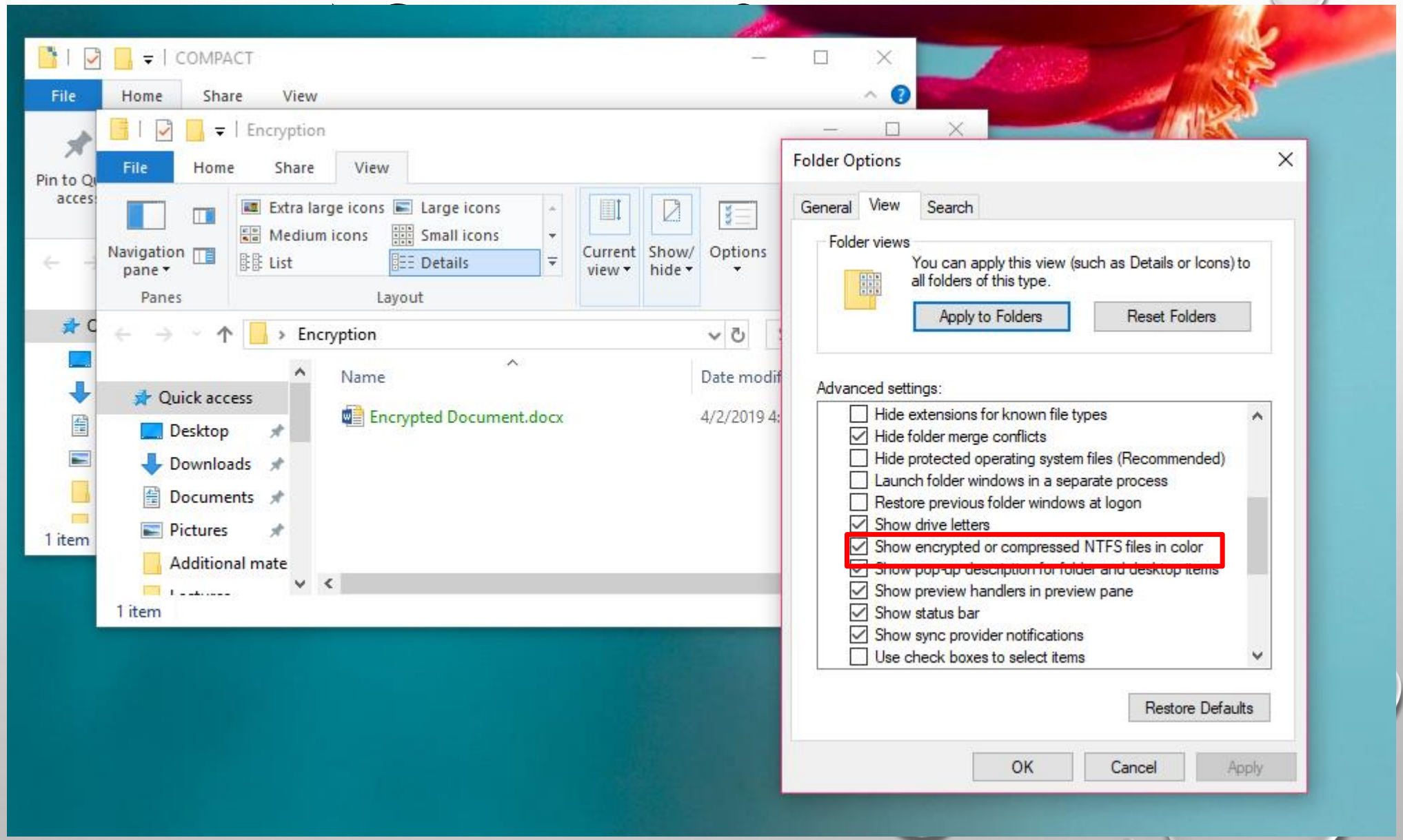
COMPRESSING FOLDER & FILES



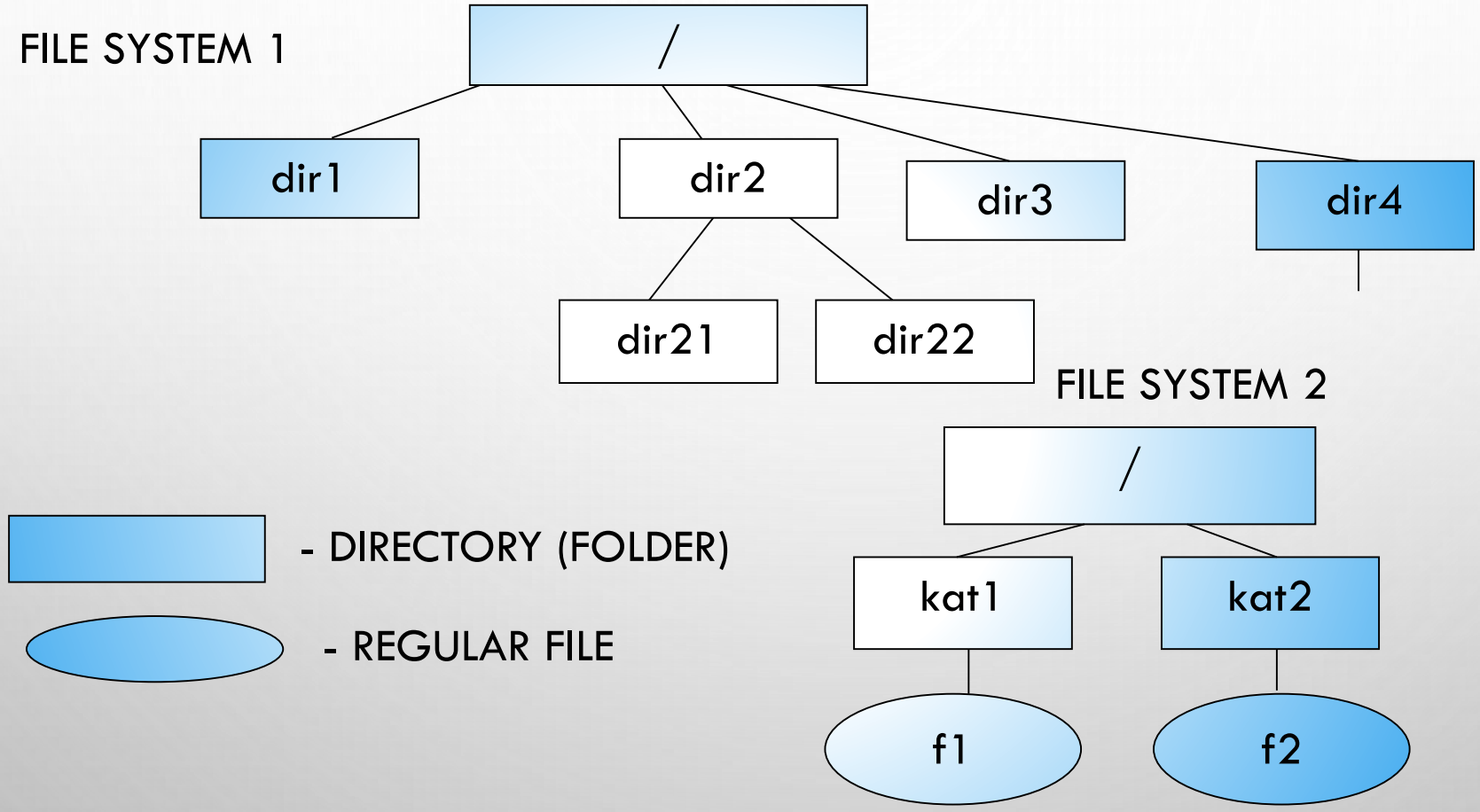
COMPRESSED FOLDER AND FILE



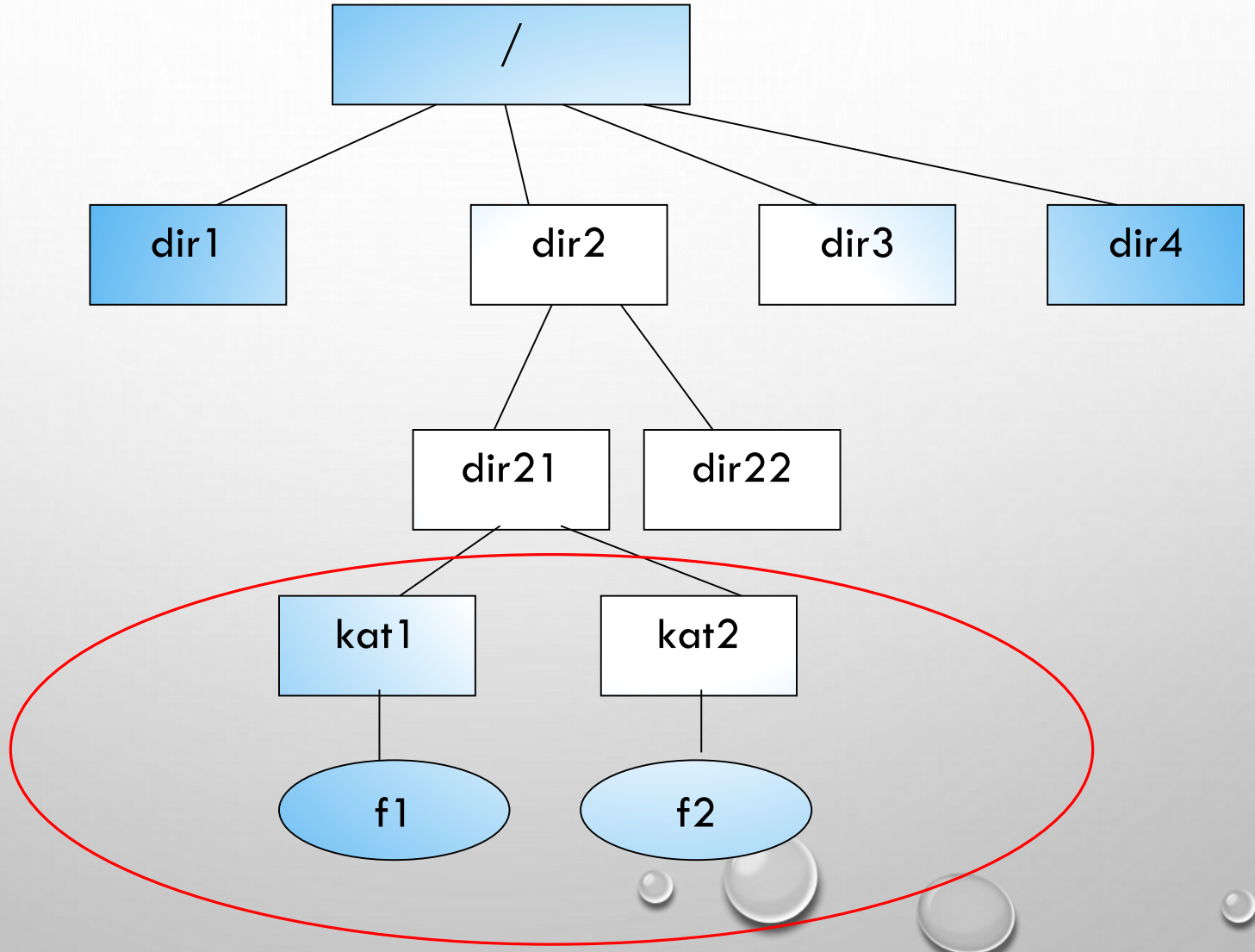
TO CHANGE COLOR OF COMPRESSED AND



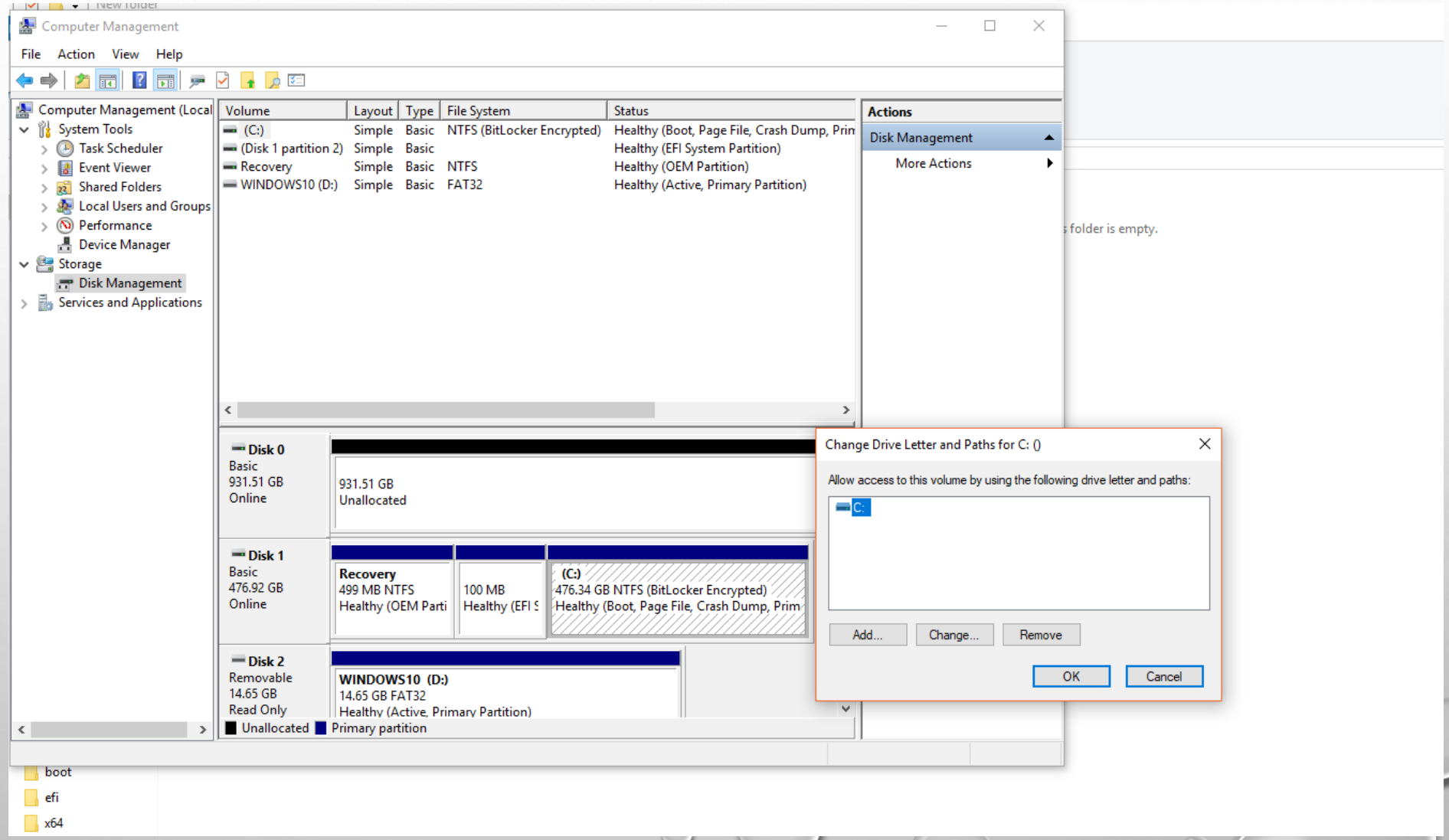
MOUNTING FILE SYSTEMS



NEW FILE SYSTEM (HAVING BEEN MOUNTED)



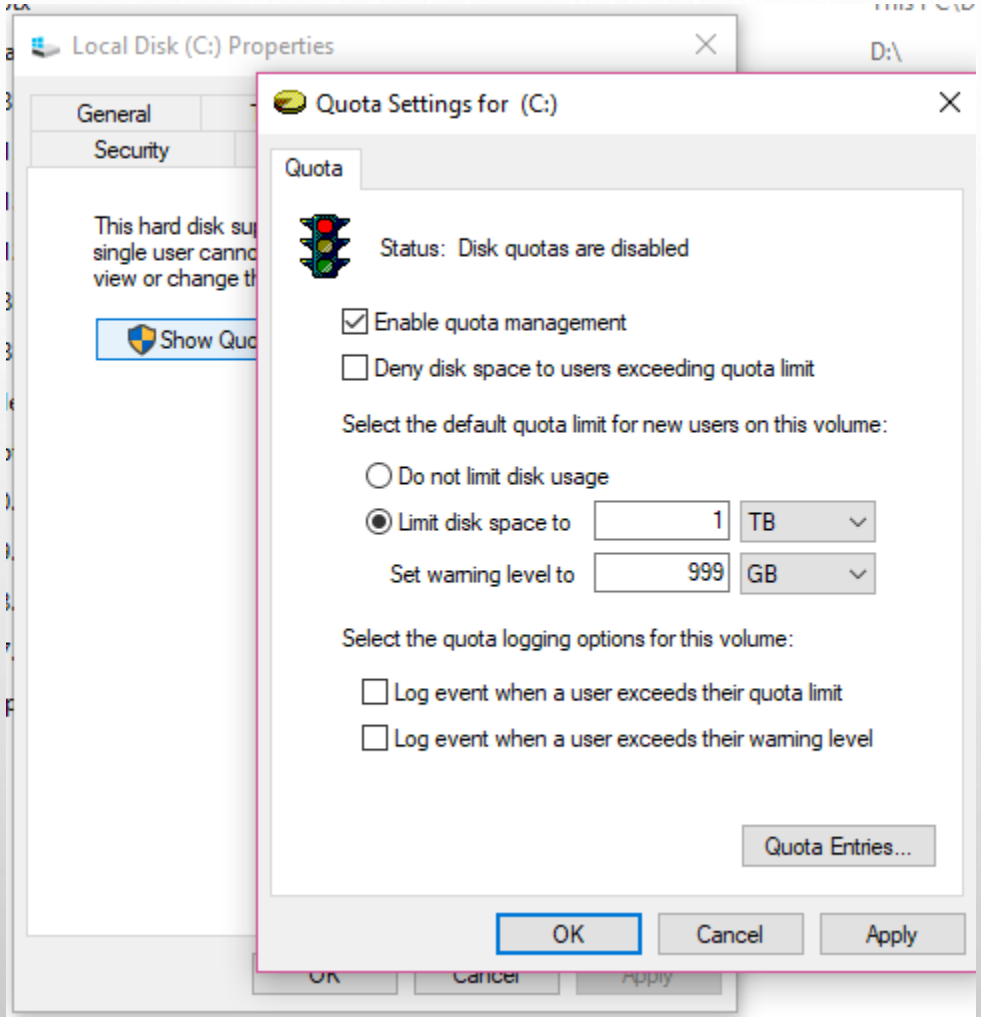
VOLUME MOUNTING IN WINDOWS



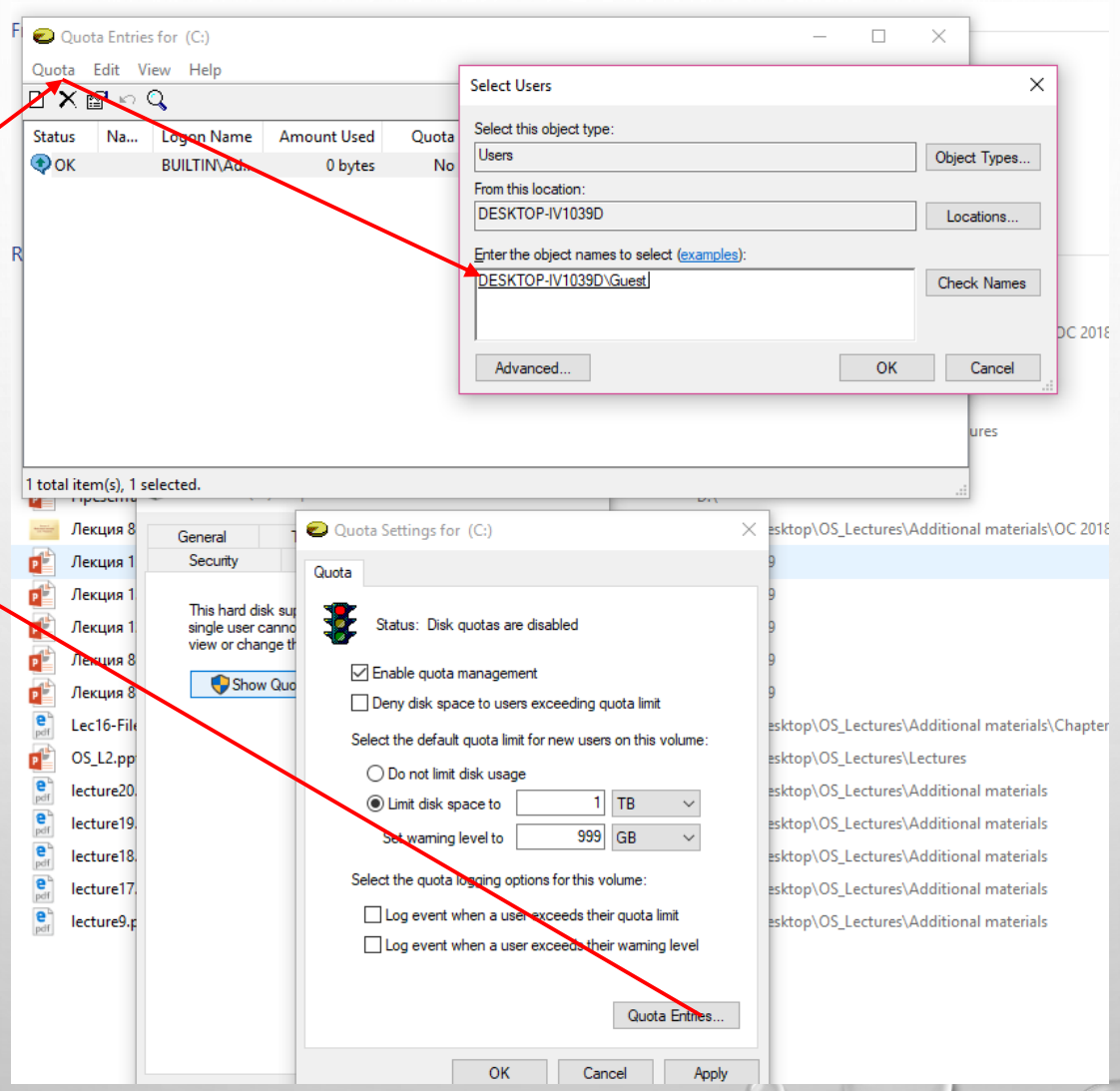
DISK QUOTA

- A **DISK QUOTA** IS A LIMIT SET FOR A SINGLE USER (OR GROUP) FOR THEIR (WHERE THEY ARE OWNERS) FILES LOCATION.
- THERE ARE TWO BASIC TYPES OF DISK QUOTAS:
  - ✓ THE FIRST, KNOWN AS A *USAGE QUOTA* OR *BLOCK QUOTA*, LIMITS THE AMOUNT OF DISK SPACE THAT CAN BE USED (REALIZED IN WINDOWS);
  - ✓ THE SECOND, KNOWN AS A *FILE QUOTA* OR *INODE QUOTA*, LIMITS THE NUMBER OF FILES AND DIRECTORIES THAT CAN BE CREATED (REALIZED IN SEVERAL VERSIONS OF LINUX).

SETTING “QUOTA”



QUOTA FOR A DEFINITE USER



NAMED STREAMS IN FILES

- STREAM IS A SEQUENCE OF BYTES.
- EVERY FILE HAS A SINGLE UNNAMED STREAM (ITS NAME IS THE SAME AS THE FILE NAME).
- IN THE MODERN VERSION OF NTFS THERE IS AN OPPORTUNITY TO CREATE ADDITIONAL **NAMED** STREAMS (THIS TYPE STREAMS HAVE THE NAME: NAME_OF_FILE:NAME_OF_STREAM)
- THE ADVANTAGE OF THIS CONCEPT: WHEN YOU COPY THIS FILE, ALL ITS STREAMS, BOTH NAMED AND UNNAMED, ARE COPIED SIMULTANEOUSLY
- FOR EXAMPLE: YOU MIGHT HAVE FILE (“MY FILE.TXT”) WITH SOME TEXT (“ HELLO WORLD!”),
- YOU CAN CREATE STREAM NAMED “DATE” AND WRITE THE CURRENT DATE THERE
- SEE THE NEXT SLIDE

Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.17134.648]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>copy con "My File.txt"
HELLO, WORLD!
^Z
        1 file(s) copied.

C:\Windows\system32>copy "My File.txt" con
HELLO, WORLD!
        1 file(s) copied.

C:\Windows\system32>date /t
Tue 04/02/2019

C:\Windows\system32>date /t > "My File.txt:date"

C:\Windows\system32>type "My File.txt"
HELLO, WORLD!

C:\Windows\system32>type "My File.txt:date"
The filename, directory name, or volume label syntax is incorrect.

C:\Windows\system32>more< "My File.txt:date"
Tue 04/02/2019

C:\Windows\system32>more< "My File.txt"
HELLO, WORLD!

C:\Windows\system32>
```

REGISTRY

REGISTRY

- THE **WINDOWS REGISTRY** IS A HIERARCHICAL DATABASE THAT STORES LOW-LEVEL SETTINGS FOR THE MICROSOFT WINDOWS OPERATING SYSTEM AND FOR APPLICATIONS THAT OPT TO USE THE REGISTRY.
- THE KERNEL, DEVICE DRIVERS, SERVICES, SECURITY ACCOUNTS MANAGER, AND USER INTERFACE CAN ALL USE THE REGISTRY. THE REGISTRY ALSO ALLOWS ACCESS TO COUNTERS FOR PROFILING SYSTEM PERFORMANCE.
- IN SIMPLE TERMS, THE REGISTRY OR WINDOWS REGISTRY CONTAINS INFORMATION, SETTINGS, OPTIONS, AND OTHER VALUES FOR PROGRAMS AND HARDWARE INSTALLED ON ALL VERSIONS OF MICROSOFT WINDOWS OPERATING SYSTEMS.
- FOR EXAMPLE, WHEN A PROGRAM IS INSTALLED, A NEW SUBKEY CONTAINING SETTINGS SUCH AS A PROGRAM'S LOCATION, ITS VERSION, AND HOW TO START THE PROGRAM, ARE ALL ADDED TO THE WINDOWS REGISTRY.

REGISTRY: KEYS & VALUES

- THE REGISTRY CONTAINS TWO BASIC ELEMENTS: **KEYS** AND **VALUES**.
- REGISTRY *KEYS* ARE CONTAINER OBJECTS SIMILAR TO FOLDERS.
- KEYS MAY CONTAIN VALUES AND SUBKEYS. KEYS ARE REFERENCED WITH A SYNTAX SIMILAR TO WINDOWS' PATH NAMES, USING BACKSLASHES TO INDICATE LEVELS OF HIERARCHY. KEYS MUST HAVE A CASE INSENSITIVE NAME WITHOUT BACKSLASHES.
- REGISTRY *VALUES* ARE NON-CONTAINER OBJECTS SIMILAR TO FILES.

REGISTRY KEYS

THERE ARE FIVE PREDEFINED ROOT KEYS, TRADITIONALLY NAMED ACCORDING TO THEIR CONSTANT HANDLES DEFINED IN THE WIN32 API, OR BY SYNONYMOUS ABBREVIATIONS (DEPENDING ON APPLICATIONS):

- HKEY_LOCAL_MACHINE OR HKLM
- HKEY_CURRENT_CONFIG OR HKCC
- HKEY_CLASSES_ROOT OR HKCR
- HKEY_CURRENT_USER OR HKCU
- HKEY_USERS OR HKU

REGISTRY KEYS: HKEY_LOCAL_MACHINE

HKEY_LOCAL_MACHINE (HKLM) - STORES SETTINGS THAT ARE SPECIFIC TO THE LOCAL COMPUTER. THE KEY LOCATED BY HKLM IS ACTUALLY NOT STORED ON DISK, BUT MAINTAINED IN MEMORY BY THE SYSTEM KERNEL IN ORDER TO MAP ALL THE OTHER SUBKEYS. APPLICATIONS CANNOT CREATE ANY ADDITIONAL SUBKEYS. ON WINDOWS NT, THIS KEY CONTAINS FOUR SUBKEYS, "SAM", "SECURITY", "SYSTEM", AND "SOFTWARE", THAT ARE LOADED AT BOOT TIME WITHIN THEIR RESPECTIVE FILES LOCATED IN THE %SYSTEMROOT%\SYSTEM32\CONFIG FOLDER. THE FIFTH SUBKEY, "HARDWARE", IS VOLATILE AND IS CREATED DYNAMICALLY, AND AS SUCH IS NOT STORED IN A FILE (IT EXPOSES A VIEW OF ALL THE CURRENTLY DETECTED PLUG-AND-PLAY DEVICES).

REGISTRY KEYS: HKEY_CLASSES_ROOT

- ABBREVIATED HKCR, HKEY_CLASSES_ROOT CONTAINS INFORMATION ABOUT REGISTERED APPLICATIONS, SUCH AS FILE ASSOCIATIONS AND OLE OBJECT CLASS IDS, TYING THEM TO THE APPLICATIONS USED TO HANDLE THESE ITEMS.
- IT IS A COMPILATION OF USER-BASED HKCU\SOFTWARE\CLASSES AND MACHINE-BASED HKLM\SOFTWARE\CLASSES. INFORMATION STORED IN THIS KEY IS NOT PERMANENTLY STORED ON DISK, BUT RATHER REGENERATED AT BOOT TIME.

REGISTRY KEYS: HKEY_CURRENT_CONFIG

- CONTAINS INFORMATION GATHERED AT RUNTIME
- INFORMATION STORED IN THIS KEY IS NOT PERMANENTLY STORED ON DISK, BUT RATHER REGENERATED AT BOOT TIME
- IT IS A HANDLE TO THE KEY "HKEY_LOCAL_MACHINE\SYSTEM\CURRENTCONTROLSET \HARDWARE PROFILES\CURRENT", WHICH IS INITIALLY EMPTY BUT POPULATED AT BOOT TIME BY LOADING ONE OF THE OTHER SUBKEYS STORED IN "HKEY_LOCAL_MACHINE\SYSTEM \CURRENTCONTROLSET\HARDWARE PROFILES”

REGISTRY KEYS: HKEY_USERS, HKEY_CURRENT_USER

- ABBREVIATED HKU, HKEY_USERS CONTAINS SUBKEYS CORRESPONDING TO THE HKEY_CURRENT_USER KEYS FOR EACH USER PROFILE ACTIVELY LOADED ON THE MACHINE, THOUGH USER HIVES ARE USUALLY ONLY LOADED FOR CURRENTLY LOGGED-IN USERS.
- ABBREVIATED HKCU, HKEY_CURRENT_USER STORES SETTINGS THAT ARE SPECIFIC TO THE CURRENTLY LOGGED-IN USER. ON WINDOWS NT SYSTEMS, EACH USER'S SETTINGS ARE STORED IN THEIR OWN FILES CALLED NTUSER.DAT AND USRCLASS.DAT INSIDE THEIR PROFILE (\USERS\%USERNAME% SUBFOLDER)

REGISTRY HIVES

- EVEN THOUGH THE REGISTRY PRESENTS ITSELF AS AN INTEGRATED HIERARCHICAL DATABASE, BRANCHES OF THE REGISTRY ARE ACTUALLY STORED IN A NUMBER OF DISK FILES CALLED ***HIVES***.
- SOME HIVES ARE VOLATILE AND **ARE NOT STORED** ON DISK AT ALL. AN EXAMPLE OF THIS IS THE HIVE OF BRANCH STARTING AT HKLM\HARDWARE. THIS HIVE RECORDS INFORMATION ABOUT SYSTEM HARDWARE AND IS CREATED EACH TIME THE SYSTEM BOOTS AND PERFORMS HARDWARE DETECTION.
- **INDIVIDUAL SETTINGS FOR USERS** ON A SYSTEM **ARE STORED IN A HIVE** (DISK FILE) PER USER. DURING USER LOGIN, THE SYSTEM LOADS THE USER HIVE UNDER THE HKEY_USERS KEY AND SETS THE HKCU (HKEY_CURRENT_USER) SYMBOLIC REFERENCE TO POINT TO THE CURRENT USER. THIS ALLOWS APPLICATIONS TO STORE/RETRIEVE SETTINGS FOR THE CURRENT USER IMPLICITLY UNDER THE HKCU KEY.
- NOT ALL HIVES ARE LOADED **AT ANY ONE TIME**. AT BOOT TIME, ONLY A MINIMAL SET OF HIVES ARE LOADED, AND AFTER THAT, HIVES ARE LOADED AS THE OPERATING SYSTEM INITIALIZES AND AS USERS LOG IN OR WHENEVER A HIVE IS EXPLICITLY LOADED BY AN APPLICATION.

REGISTRY HIVES: DISK LOCATION

This PC › Local Disk (C:) › Windows › System32 › config

Search con

Quick access
Desktop
Downloads
Documents
Pictures
Lectures
PDF Lectures
students
System32
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Network

Name	Date modified	Type	Size
BCD-Template.LOG	2/20/2019 8:38 AM	Text Document	
COMPONENTS	3/31/2019 9:24 AM	File	4
COMPONENTS.LOG1	4/11/2018 2:04 PM	LOG1 File	
COMPONENTS.LOG2	4/11/2018 2:04 PM	LOG2 File	1
COMPONENTS{8ebe95e2-3dcb-11e8-a9...	3/16/2019 4:24 AM	BLF File	
COMPONENTS{8ebe95e2-3dcb-11e8-a9...	2/20/2019 1:48 AM	REGTRANS-MS File	
COMPONENTS{8ebe95e2-3dcb-11e8-a9...	3/16/2019 4:24 AM	REGTRANS-MS File	
DEFAULT	3/24/2019 12:43 AM	File	
DEFAULT.LOG1	4/11/2018 2:04 PM	LOG1 File	
DEFAULT.LOG2	4/11/2018 2:04 PM	LOG2 File	
DRIVERS	4/6/2019 1:36 AM	File	
DRIVERS.LOG1	4/11/2018 2:04 PM	LOG1 File	
DRIVERS.LOG2	4/11/2018 2:04 PM	LOG2 File	
DRIVERS{8ebe95e8-3dcb-11e8-a9d9-7cfe...	3/16/2019 4:10 AM	BLF File	
DRIVERS{8ebe95e8-3dcb-11e8-a9d9-7cfe...	3/16/2019 4:10 AM	REGTRANS-MS File	
DRIVERS{8ebe95e8-3dcb-11e8-a9d9-7cfe...	2/20/2019 8:39 AM	REGTRANS-MS File	
ELAM	2/20/2019 8:39 AM	File	
ELAM.LOG1	4/11/2018 2:04 PM	LOG1 File	
ELAM.LOG2	4/11/2018 2:04 PM	LOG2 File	
ELAM{8ebe9616-3dcb-11e8-a9d9-7cfe90...	2/20/2019 8:39 AM	BLF File	
ELAM{8ebe9616-3dcb-11e8-a9d9-7cfe90...	2/20/2019 8:39 AM	REGTRANS-MS File	
ELAM{8ebe9616-3dcb-11e8-a9d9-7cfe90...	2/20/2019 8:39 AM	REGTRANS-MS File	
SAM	3/24/2019 12:43 AM	File	
SAM.LOG1	4/11/2018 2:04 PM	LOG1 File	
SAM.LOG2	4/11/2018 2:04 PM	LOG2 File	
SECURITY	3/24/2019 12:43 AM	File	
SECURITY.LOG1	4/11/2018 2:04 PM	LOG1 File	
SECURITY.LOG2	4/11/2018 2:04 PM	LOG2 File	

46 items

This PC › Local Disk (C:) › Users › admin ›

Search admin

Quick access
Desktop
Downloads
Documents
Pictures
Lectures
PDF Lectures
students
System32
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Network

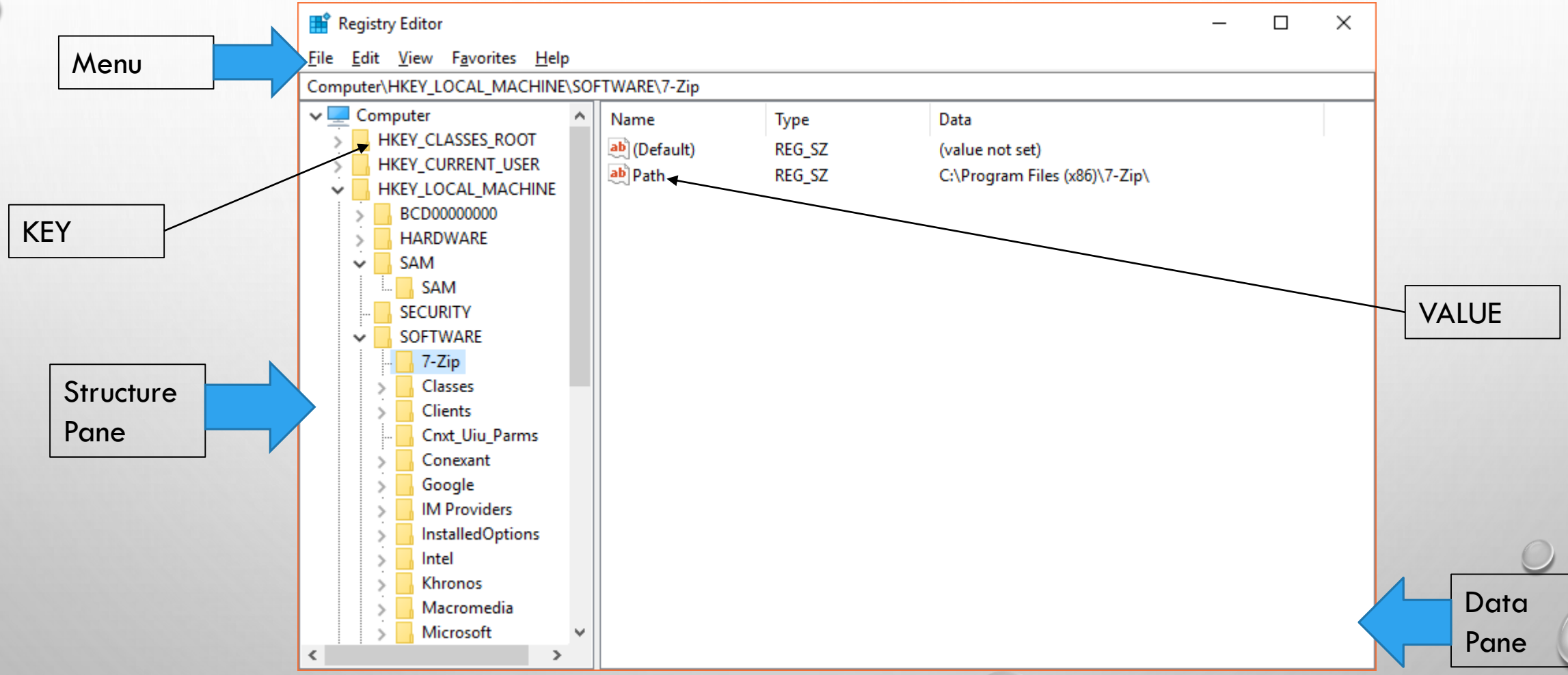
Name	Date modified	Type	Size
Documents	3/3/2019 1:04 AM	File folder	
Downloads	3/31/2019 9:44 AM	File folder	
Examples	3/31/2019 9:28 AM	File folder	
Favorites	2/20/2019 4:13 AM	File folder	
IntelGraphicsProfiles	4/6/2019 12:10 AM	File folder	
Links	2/20/2019 4:13 AM	File folder	
Local Settings	2/20/2019 1:11 AM	File folder	
MicrosoftEdgeBackups	2/20/2019 1:12 AM	File folder	
Music	2/20/2019 4:13 AM	File folder	
My Documents	2/20/2019 1:11 AM	File folder	
NetHood	2/20/2019 1:11 AM	File folder	
OneDrive	3/31/2019 9:24 AM	File folder	
Pictures	2/20/2019 4:13 AM	File folder	
PrintHood	2/20/2019 1:11 AM	File folder	
Recent	2/20/2019 1:11 AM	File folder	
Saved Games	2/20/2019 4:13 AM	File folder	
Searches	2/20/2019 4:13 AM	File folder	
SendTo	2/20/2019 1:11 AM	File folder	
Start Menu	2/20/2019 1:11 AM	File folder	
Templates	2/20/2019 1:11 AM	File folder	
Videos	3/29/2019 1:25 AM	File folder	
NTUSER.DAT	4/4/2019 4:44 AM	DAT File	2,304 KB
ntuser.dat.LOG1	2/20/2019 1:11 AM	LOG1 File	908 KB
ntuser.dat.LOG2	2/20/2019 1:11 AM	LOG2 File	604 KB
NTUSER.DAT{8ebe95f7-3dcb-11e8-a9d9-...	2/20/2019 1:12 AM	BLF File	64 KB
NTUSER.DAT{8ebe95f7-3dcb-11e8-a9d9-...	2/20/2019 1:12 AM	REGTRANS-MS File	512 KB
NTUSER.DAT{8ebe95f7-3dcb-11e8-a9d9-...	2/20/2019 1:12 AM	REGTRANS-MS File	512 KB
ntuser.ini	2/20/2019 1:11 AM	Configuration sett...	1 KB

42 items 1 item selected 2.25 MB

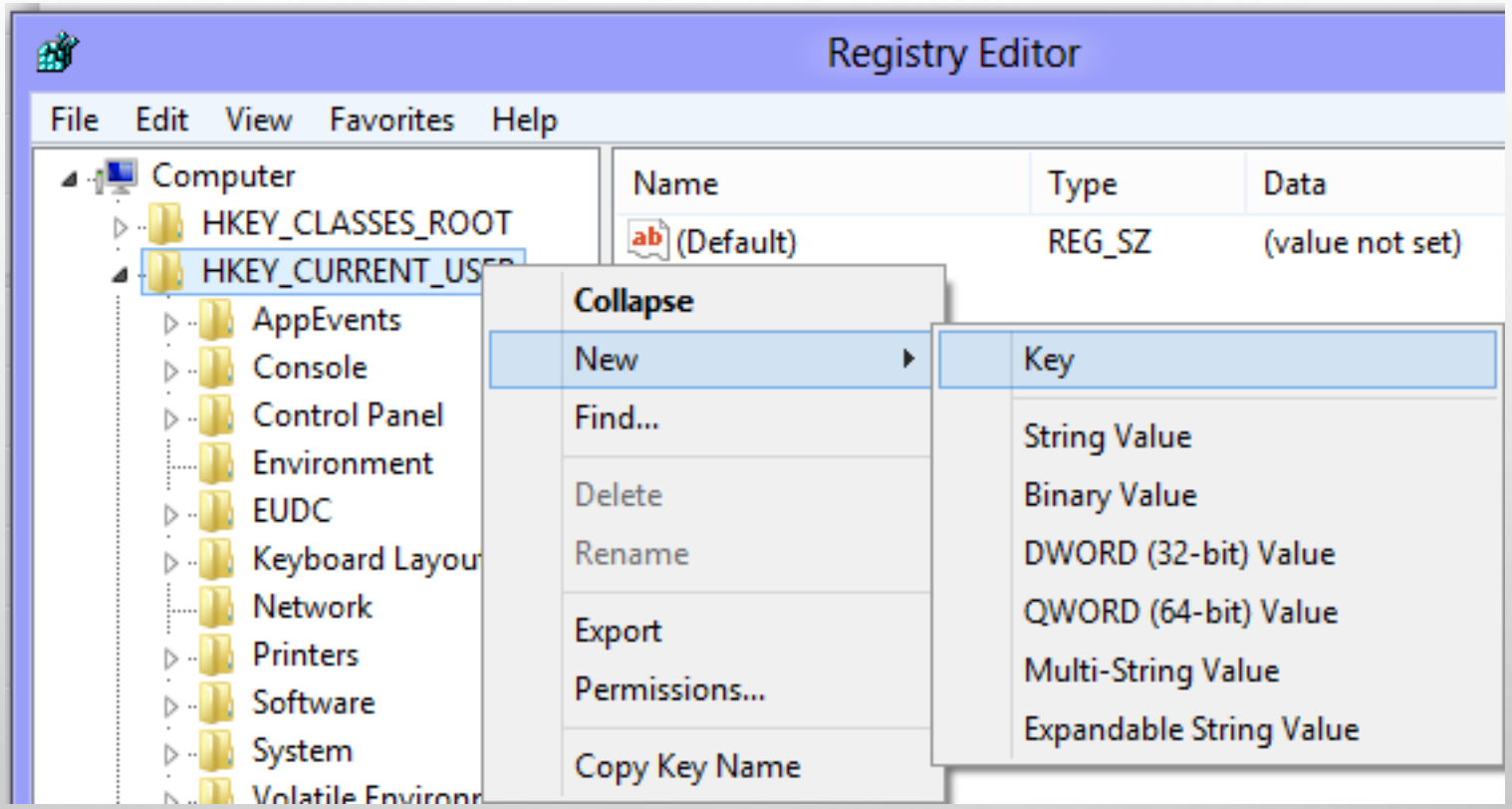
REGISTRY EDITOR

- THE MAIN PURPOSE OF REGISTRY EDITOR IS TO VIEW AND CHANGE THE SETTINGS IN THE SYSTEM REGISTRY
- PRESS WIN+R KEYS ON YOUR KEYBOARD, THE "RUN" DIALOG WILL APPEAR. TYPE **REGEDIT** WITHOUT QUOTES AND PRESS ENTER

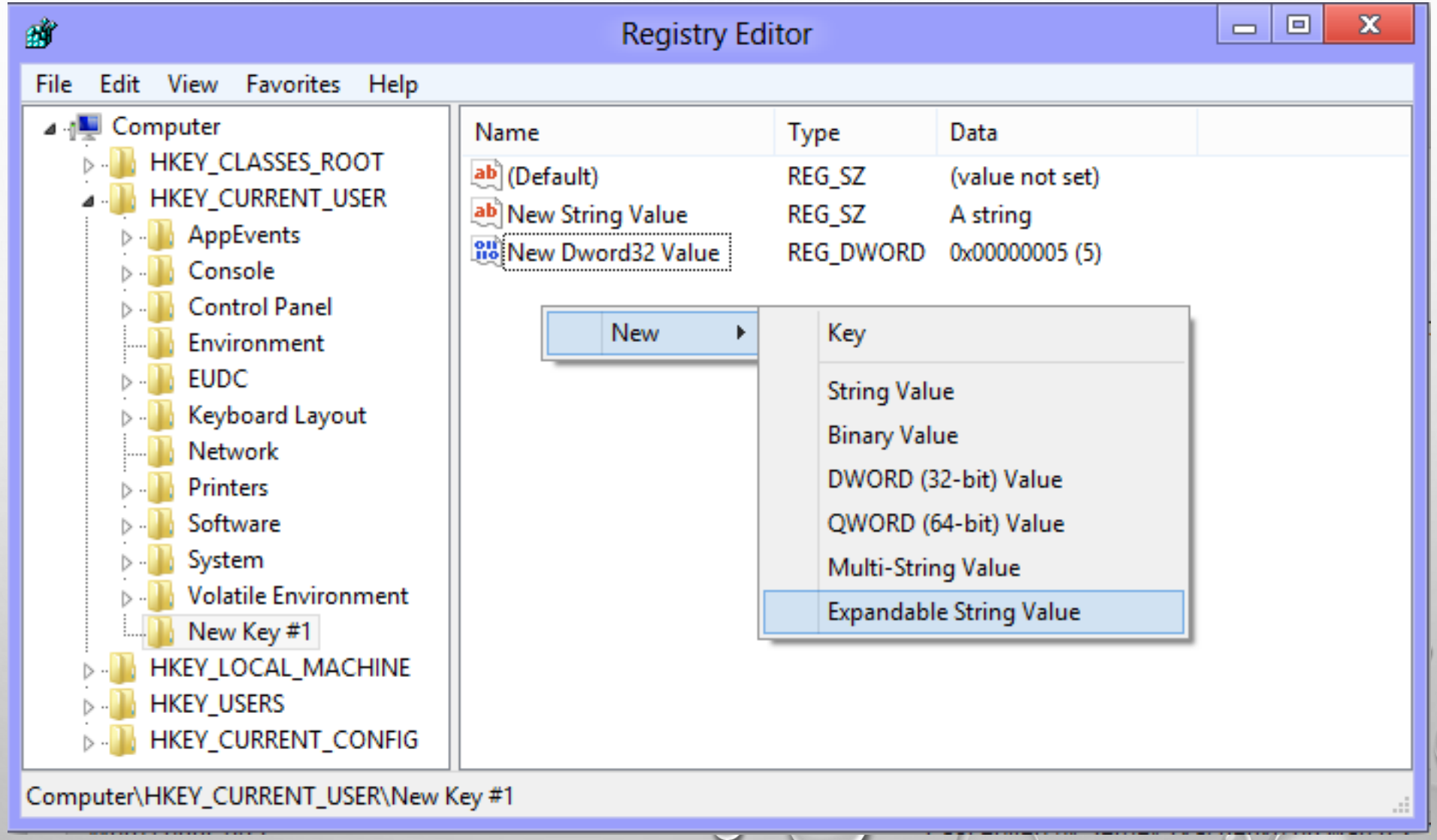
REGISTRY EDITOR WINDOW



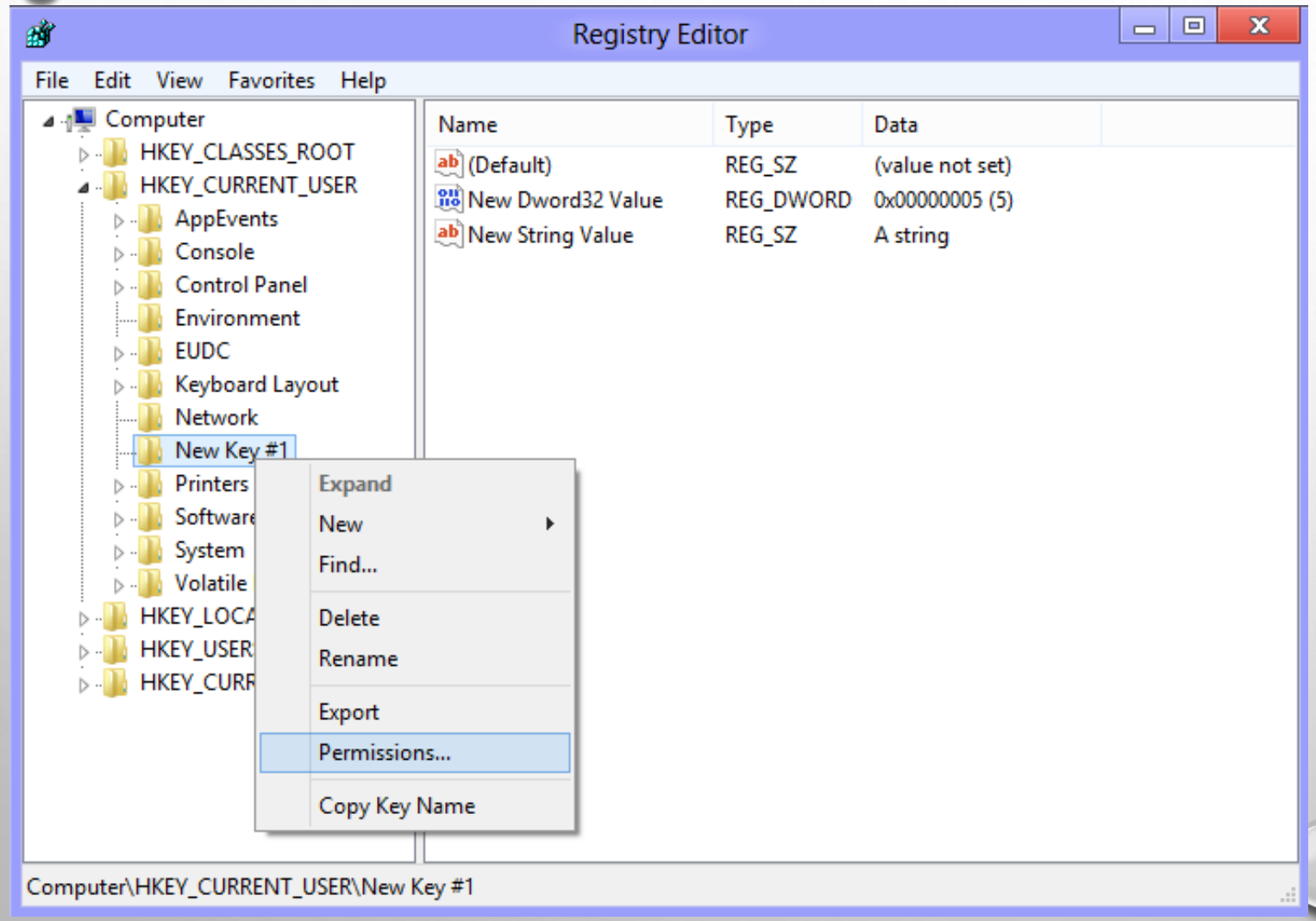
CREATING A NEW KEY

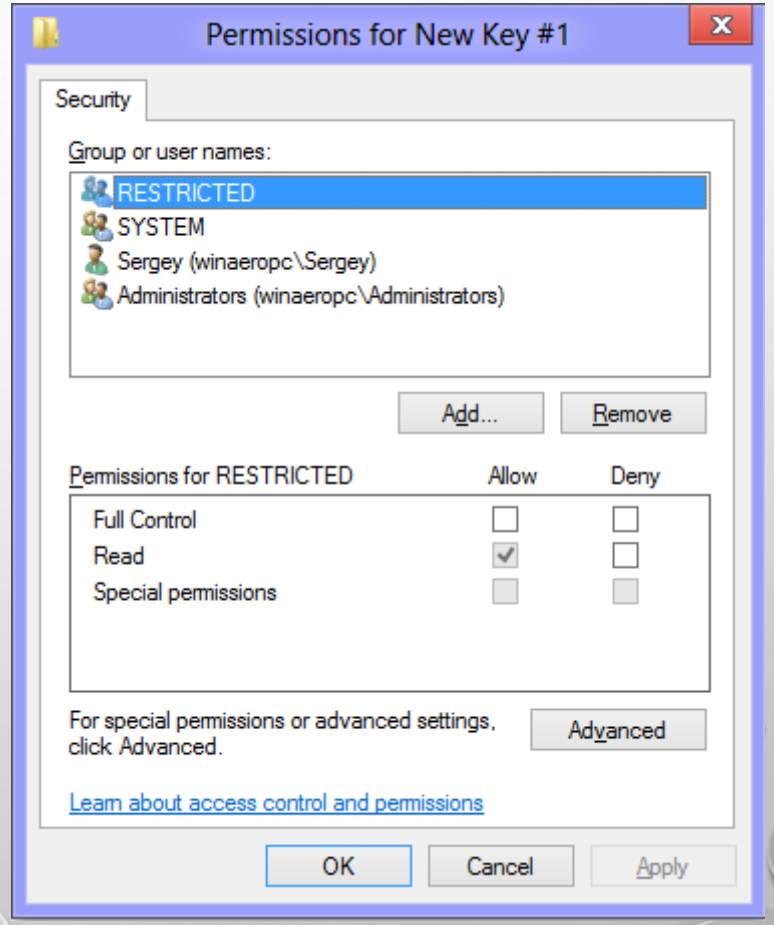


CREATING A NEW VALUE

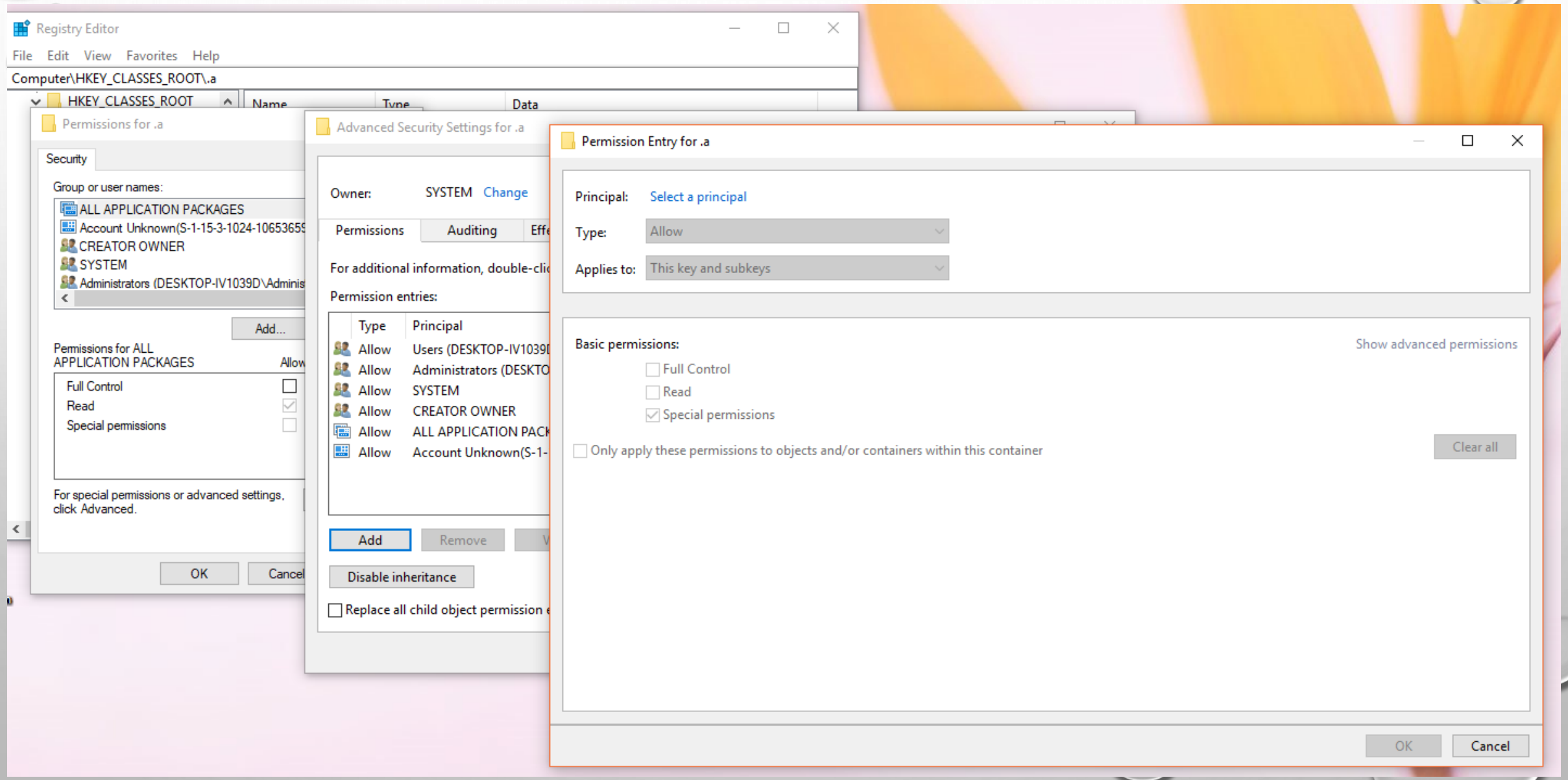


PERMISSIONS SETTING

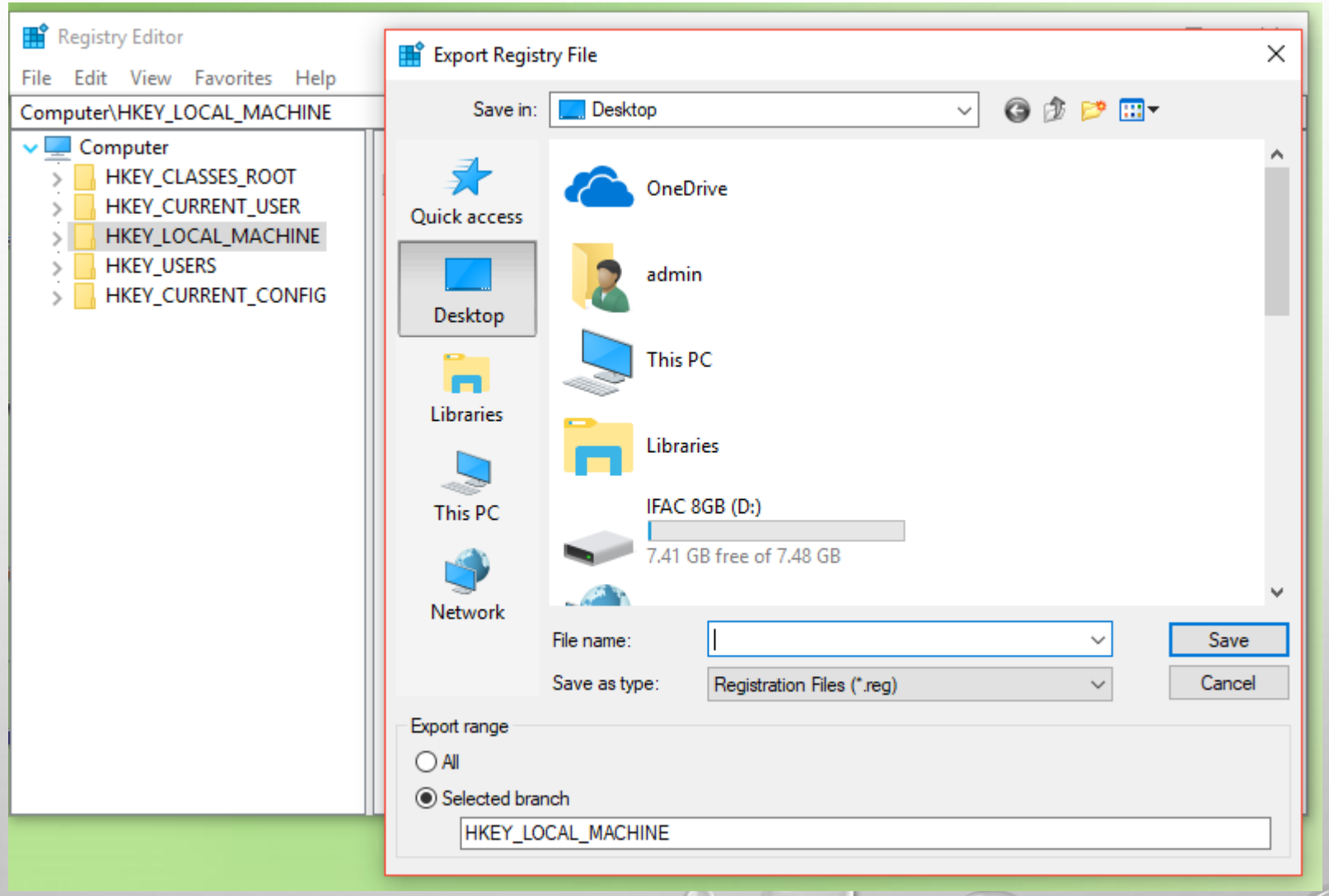




AUDIT SETTINGS



EXPORT INTO THE REG FILE



.REG FILES

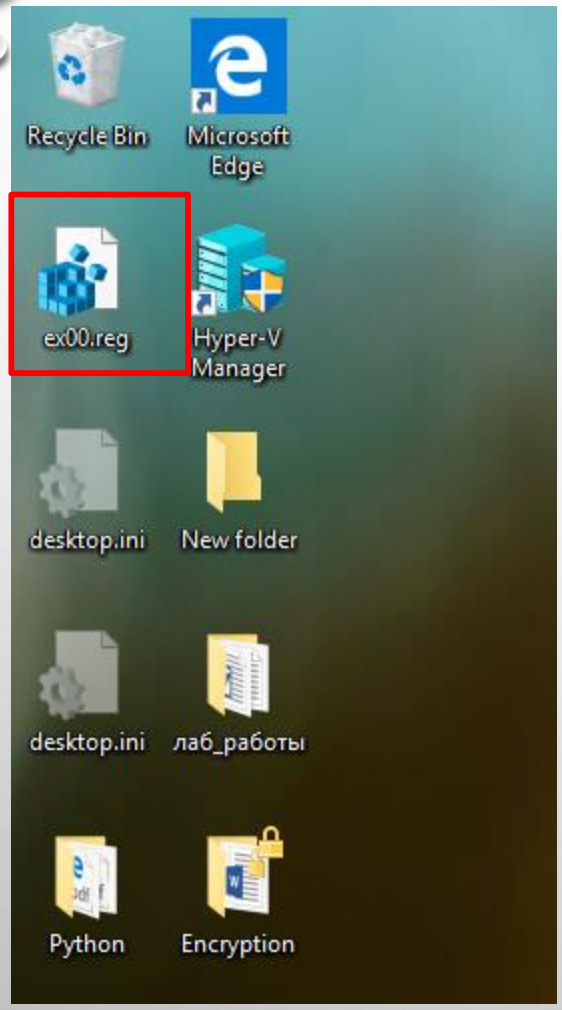
- ARE TEXT-BASED HUMAN-READABLE FILES FOR EXPORTING AND IMPORTING PORTIONS OF THE REGISTRY
- SYNTAX OF REG FILES: CONSISTS OF THE FOLLOWING STRUCTURES

[HIVE_NAME\KEY_NAME\SUBKEY_NAME]

"VALUE_NAME"=VALUE_TYPE:VALUE_DATA

- DATA FROM THE REG FILES CAN BE ADDED/MERGED WITH THE REGISTRY BY DOUBLE-CLICKING THESE FILES OR USING "REG" COMMAND WITH THE /S SWITCH IN THE COMMAND LINE

REG FILES



ex01.reg - Notepad

File Edit Format View Help

```
Windows Registry Editor Version 5.00

[HKEY_CLASSES_ROOT\.xlsx]
"Content Type"="application/vnd.openxmlformats-officedocument.spreadsheetml.sheet"
@="Excel.Sheet.12"
"PerceivedType"="document"

[HKEY_CLASSES_ROOT\.xlsx\Excel.Sheet.12]

[HKEY_CLASSES_ROOT\.xlsx\Excel.Sheet.12\ShellNew]
"FileName"="excel12.xlsx"

[HKEY_CLASSES_ROOT\.xlsx\PersistentHandler]
@="{4887767F-7ADC-4983-B576-88FB643D6F79}"

[HKEY_CLASSES_ROOT\.xlsx\ShellEx]

[HKEY_CLASSES_ROOT\.xlsx\ShellEx\PropertyHandler]
@="{993BE281-6695-4BA5-8A2A-7AACBFAAB69E}"

[HKEY_CLASSES_ROOT\.xlsx\ShellEx\{8895b1c6-b41f-4c1c-a562-0d564250836f}]
@="{00020827-0000-0000-C000-000000000046}"

[HKEY_CLASSES_ROOT\.xlsx\ShellEx\{BB2E617C-0920-11d1-9A0B-00C04FC2D6C1}]
@="{C41662BB-1FA0-4CE0-8DC5-9B7F8279FF97}"
```

SEARCH FOR A KEY/VALUE