Congratulations! You passed!

Grade received 92.59% **Latest Submission Grade** 92.59% **To pass** 80% or higher

Go to next item

1. The Windows Registry is defined as — 0 / 1 point

- ○ Flat file
- ○ SQL database
- ○ Central hierarchical database
- ◉ Central relational database

Incorrect

2. The Windows Registry replaced which type of file? — 1 / 1 point

- ◉ Configuration and Initialization files
- ○ Property lists
- ○ Link Files
- ○ Log Files

Correct
The Windows Registry replaced the configuration and initialization (ini) files used in Windows versions prior to Windows NT

3. What information is NOT contained in the Windows Registry? — 1 / 1 point

- ◉ Disk structure information
- ○ System Information
- ○ Application specific information
- ○ user information

Correct
The windows registry contains user information, system information and application specific information.

4. The Windows Registry can be useful for? — 1 / 1 point

- ○ Determining cluster size
- ◉ Validating findings through an investigation
- ○ looking up a phone number
- ○ Determining the number of partitions on a drive

Correct
The registry can be used to validate OS install date and time, last logged-on user, and much more.

5. The Windows Registry is important because it records? — 1 / 1 point

- ○ applications and installed programs
- ○ user account information
- ○ system information

- [x] all of these

Correct
The windows registry contains user information, system information and program and application specific information.

6. The type of case you are investigating... **1 / 1 point**

- [ ] only matters if it is a Windows 7 computer
- [ ] has nothing to do with the registry
- [ ] will NOT determine the type of information you are looking for
- [x] will determine the type of information you are looking for

Correct
The type of case you are investigation will always determine the type of information you are looking for.

7. The Windows Registry contains **1 / 1 point**

- [ ] Keys
- [ ] Values
- [ ] Sub-Keys
- [ ] Data
- [ ] Hives
- [x] All of these

Correct
The registry is made up of hives, keys, subkeys, and data.

8. The registry hive files are pulled into memory, handle keys, and represented as **1 / 1 point**

- [ ] File Keys (FK)
- [ ] Block Keys (BK)
- [x] Handle Keys (HK)
- [ ] user Keys (UK)

Correct
The Hive Files are pulled into memory , Handel Keys represented as “HK”.

9. Which Registry Key is only found on a live running system? **1 / 1 point**

- [ ] Sam
- [ ] Security
- [ ] System
- [x] Hardware
- [ ] Software

Correct
HKey_Current User, Hardware, and HK_Current_Config are only found on a live running system.

10. Registry values can be in several different forms. Which is not a registry value form? **1 / 1 point**

- (●) SQL Data
- ( ) String Data
- ( ) Binary Data
- ( ) Hex Data

✓ **Correct**
Registry Values can be in several different forms, Binary Data, String Data, and Hex Data.

11. The user specific registry files contained in the registry are? **1 / 1 point**

- ( ) Amcache and Sam
- (●) NTUser.Dat and UsrClass.Dat
- ( ) None of the above
- ( ) PTUser.reg and user.Dat

✓ **Correct**
User Files specific files contained with the registry are NT User.dat, and User Class.dat

12. The system specific files contained within the registry are? **1 / 1 point**

- ( ) security
- ( ) AmCache
- ( ) Sam
- ( ) software
- (●) All of these
- ( ) system

✓ **Correct**
System specific files contained with the registry are, Sam, System, Security, Software, AmCache.

13. The Sam, Security, Software, and System Registry files are located at **1 / 1 point**

- (●) Volume root\Windows\system32\config
- ( ) Volume root\WindowsNT\system32\config
- ( ) Volume root\Windows\Sam\config
- ( ) Volume root\system32\user\config

✓ **Correct**
The path to Sam, system, Security, and Software registry hive files.

14. What are the two registry files that relate to a specific user? **1 / 1 point**

- ( ) Sam and System
- ( ) Sam and Security
- (●) NTUser.dat and USRClass.dat

- ○ NTUser.dat and Software

✓ **Correct**
Each user on a windows system will have their own NTUser.dat and USRClass.dat. Which relates to that specific user.

15. Registry browser is a **1 / 1 point**

- ○ Older type of Windows registry prior to Windows 95
- ○ Hex editor
- ○ Registry hive sub-key
- ◉ Specialized tool used to view the Window Registry

✓ **Correct**
Registry Browser is a specialized tool used to view the Window Registry.

16. Which sub-key is used to determine the current control set? **1 / 1 point**

- ◉ Select
- ○ Microsoft
- ○ System
- ○ Windows

✓ **Correct**
The select sub-key is used to determine the current control set.

17. What registry hive file contains the the time zone setting **1 / 1 point**

- ○ Sam
- ◉ System
- ○ Security
- ○ Software

✓ **Correct**
The System sub-key contains the time zone setting.

18. The Windows OS Version and Install date are contained in the ____ registry hive? **1 / 1 point**

- ○ System
- ◉ Software
- ○ Security
- ○ Sam

✓ **Correct**
The Windows OS Version and Install date are contained in the Software registry hive.

19. Regarding the live Windows Registry, which two hive keys or sub keys only exists in the live registry? **1 / 1 point**

- ○ None of these
- ◉ Both A and B
- ○ HKEY_LOCAL_MACHINE-SYSTEM SUBKEY
- ○ HKEY_LOCAL_MACHINE-SAM SUBKEY
- ○ HKEY_LOCAL_MACHINE—HARDWARE SUBKEY

- HKEY_CURRENT_USER

Correct
HKEY_CURRENT_USER (Information for the currently logged on user) (NTuser.dat file-for that specific user)HKEY_LOCAL_MACHINE—HARDWARE SUBKEY (hardware attached to the system such as the CPU, keyboard, mouse, hard drives, etc.) populated when the system boots up.

20. Which two Registry files are not accessible on a live running computer. As seen in Regedit. **1 / 1 point**

- (•) Both Sam and security
- ( ) security
- ( ) Both Security and software
- ( ) system
- ( ) Sam
- ( ) software

Correct
Sam and Security are not accessible on a live running system using regedit.

21. What Registry sub key contains a list of recently used documents by file extension? **1 / 1 point**

- (•) Recent Docs subkey
- ( ) User Assist
- ( ) The Run Sub Once subkey
- ( ) The Run MRU subkey

Correct
Sam and Security are not accessible on a live running system using regedit.

22. The typed URL subkey contains: **1 / 1 point**

- (•) Web Addresses typed into the Internet Explorer Address Bar
- ( ) Recently run applications
- ( ) Programs run at startup
- ( ) Search terms typed into Windows Explorer

Correct
Typed URLs subkey located in the Nt user.dat hive file Populated when a user types a URL into the internet Explorer address bar. And with URLs completed by the browser's AutoComplete functionality, choosing a url in the drop down menu.

23. The values in which key are stored using ROT13 **1 / 1 point**

- ( ) Typed URLs
- ( ) Run
- ( ) Recent Applications
- (•) User Assist

Correct
User assist subkey Registry values under these subkeys are obfuscated using ROT-13 which basically substitutes a character with another character 13 position away from it in the alphabet.

24. This sub key tracks recently used applications and may contain a record of the files that were opened with each application... **0 / 1 point**

- ( ) User Assist

- User Assist
- Recent Apps
- Run MRU
- Run Once

Incorrect

25. This subkey tracks user specific, persistent, applications that are set to run at start up? 1 / 1 point

- Run Once
- Run
- Run MRU
- Recent Apps

Correct
The Run subkey tracks persistent applications/programs that are set to run at startup. The subkey is executed when the specific user logs onto the system – Auto start location.

26. This key tracks files that have been opened or saved within a Windows Open/Save dialog box. This includes web browsers and commonly used applications? 1 / 1 point

- Recent Docs
- Recent Apps
- Run MRU
- ComDlg32 OpenSavePidMRU

Correct
ComDlg32 OpenSavePidMRU This key tracks files that have been opened or saved within a Windows Open/Save dialog box. This includes web browsers and commonly used applications.

27. This key maintains a list of all the values typed into the Run box on the Start menu? 1 / 1 point

- WordWheel Query
- Run
- Run Once
- Run MRU

Correct
The Run MRU subkey maintains a list of all the values typed into the Run box on the Start menu.

28. The subkey Typed Paths does what? 1 / 1 point

- comdlg 32
- Keeps track of Files, Directories, or programs accessed by typing a File path into Windows Explorer
- Keeps track of URL typed into the Internet Explorer Address Bar
- Runs at startup

Correct
The subkey Typed Paths maintains a record of Files, Directories, or programs accessed by typing a File path into Windows Explorer.

29. Microsoft Office MRU are... 1 / 1 point

- created when a user types a path to a directory, file or application into the windows explorer.
- User specific programs that are set to run at startup with no interaction from

- [ ] user specific programs that are set to run at startup with no interaction from
- [x] Recently used Microsoft Office Documents
- [ ] programs or applications launched through the windows run box

Correct
Microsoft Office MRU sub key track recently accessed files opened with a specific application. There is also a file time, and a full path to the file or directory that was accessed. This path includes the file name.

30. What subkey tracks user key word searches? **1 / 1 point**

- [ ] ComDlg32
- [ ] Recent Apps
- [ ] Run MRU
- [x] WordWheel query

Correct
WordWheel query In windows 10 tracks search terms (user searches) that were performed using the Windows Explorer, not the taskbar search box this is handled by Cortana and these searches are not stored in the Registry. Stored in a database outside the registry.

31. The SAM file stores what information? **1 / 1 point**

- [ ] Programs set to Run at startup by a user
- [x] information about each user such as login information, login password hashes, and group information
- [ ] Information about files and applications recently accessed by a user
- [ ] information about the users internet accounts and browser history

Correct
The SAM file stores and organizes information about each user such as login information, login password hashes, and group information.

32. The Security identifier SID is comprised of 3 parts... **1 / 1 point**

- [ ] user name - Profile path- User directory
- [ ] All of the above
- [x] Issuing authority- Machine/domain identifier- Relative identifier
- [ ] Issuing identifier-Domain authority-Machine identifier

Correct
The security identifier has 3 parts: Issuing authority- Machine/domain identifier- Relative identifier.

33. The Machine identifier of the local machine is found in the ____ subkey **1 / 1 point**

- [ ] Groups
- [ ] Domains
- [x] Account
- [ ] Users

Correct
The last 12 bytes of the V value within the accounts subkey, under Sam\domains\Accounts contains the local machine identifier.

34. The relative identifier or RID identifies a? **1 / 1 point**

- [x] User
- [ ] Machine

- Group
- Domain

Correct
Relative Identifier (RID - identifying a specific user)

35. The Names subkey identifier the user's name and _____ ? 1 / 1 point

- (•) Relative Identifier
- ( ) last logon time
- ( ) password hash
- ( ) log on count

Correct
The names subkey shows the hex and decimal relative identifier (RID) of the user.

36. The last logon time is stored in the ___ subkey? 1 / 1 point

- (•) User
- ( ) Names
- ( ) Domains
- ( ) Accounts

Correct
Each user subkey has both an F and a V value and they contain all the information for each user account, such as log on times and log on count, and last failed logon.

37. The V value of the users subkey contains? 0 / 1 point

- ( ) number of failed logon's
- ( ) last logon date and time
- (•) log on count
- ( ) username and password hash

Incorrect

38. What is the function of the RunMRU subkey in the Software Hive File? 1 / 1 point

- ( ) This key shows programs that run at startup
- (•) This key maintains a list of all the values typed into the Run box on the Start menu
- ( ) This key tracks user searches
- ( ) all of the above

Correct
The RunMRU key tracks and maintains a list of all the values typed into the Run box on the Start menu.

39. The OpenSavePidMRU sub-key, which is a sub-key of Comdlg 32 tracks ... ? 1 / 1 point

- ( ) AutoStart locations
- ( ) values typed into the Run box on the Start menu
- (•) A specific executable used to open the files

- ○ User logon information and last logged on user

✓ **Correct**
Comdlg 32 Tracks the specific executable used to open the files in the OpenSavePidMRU sub-key

40. Information indicating the last logged on user would be found in which sub-key within the software hive file? **1 / 1 point**

- ○ Classes
- ○ Comdlg 32
- ◉ LogonUI
- ○ Run

✓ **Correct**
LogonUI sub-key stores information regarding the last logged on user.

41. _____ is an autostart location in the Software Hive File. **1 / 1 point**

- ○ Comdlg 32
- ◉ Run Key
- ○ Installed printers
- ○ RunMRU

✓ **Correct**
The Run Key located in the Software is an AutoStart location, meaning that it is a System wide settings for program set to run at startup with little Or no interaction from the user.

42. Windows OS install date and time would be found in the Software file in which sub-key? **1 / 1 point**

- ○ Run Once
- ○ Winlogon
- ○ Windows
- ◉ Current Version

✓ **Correct**
Location of OS Install Date and Time Microsoft\WindowsNT\CurrentVersion

43. The network list sub-keys profiles and signatures contain what information? **1 / 1 point**

- ○ User account information
- ◉ Wireless network dates and times and gateway MAC address
- ○ Domain user account information
- ○ Evidence of program execution

✓ **Correct**
Under the NetworkList subkey are two other subkeys of interest: Profiles and Signatures. The Profiles subkey contains network information stored by GUID, such as the date first connected and the date last connected.

44. In the software hive file, what 2 sub-keys contain information regarding the connection of USB devices? **0 / 1 point**

- ◉ USBStore and USB
- ○ Mountpoints and Mountspoints2
- ○ Devices and EMD Management

- Mountpoints2 and RunMRU

Incorrect

45. What key within the system file is used to determine the current control set? 1 / 1 point

- Prefetch
- Select
- Services
- Control

Correct
The select key is used to determine the current control set.

46. The last shutdown time is found within which sub-key in the system hive file? 1 / 1 point

- USBstore
- select
- Windows
- control

Correct
The last shutdown time is stored in the system file within the Windows subkey. It is stored in the windows 64bit little endian format.

47. In the system hive, the Windows services sub-key tracks programs that ___? 1 / 1 point

- Tracks USB Devices
- Indicates when the system needs service
- run automatically when the system is booted, and are started by the system and with no interaction from the user
- is not a subkey in the system hive

Correct
Windows services (referred to in the Linux world as “daemons”) are programs that run automatically when the system is booted, and are started by the system and with no interaction from the user.

48. What subkey in the system hive file contains settings for the prefetch utility? 1 / 1 point

- Select
- prefetchParameters
- Windows
- Controlset

Correct
The Prefetch Parameters subkey contains settings for the Prefetch utility. Prefetch monitors applications and files as they are launched.

49. The setting within the system hive file that controls whether or not the page file is cleared at shutdown is ___? 1 / 1 point

- select
- Memory Management

- shutdown
- Crash Control

Correct
The setting to clear or not to clear the page file at shutdown is located in the System hive file at this file path ControlSet\Control\Session Manager\Memory Management.

50. What type of information is found at this location in the System hive file

1 / 1 point

Location:ControlSet001\Enum\USBSTOR\"Device"\"Serial# or Unique instance ID"\Properties\{83da6326-97a6-4088-9453-a1923f573b29}

- (•) USB device connection and disconnection dates and times
- ( ) user account information
- ( ) prefetch settings
- ( ) programs set to run at startup

Correct
Subkey Name: Properties (under USB Store) Location:ControlSet001\Enum\USBSTOR\"Device"\"Serial# or Unique instance ID"\Properties\{83da6326-97a6-4088-9453-a1923f573b29} First Install Date and Time: Date and time when the device was first installed. 0x 0064, Last Install Date and Time: Last date and time that the device drivers were installed or updated. 0x 0065, Last Arrival Date and Time: Last date and time that the device was connected to the system. 0x 0066, Last Removal Date and Time: Last date and time that the device was removed from the system. 0x 0067

51. Appcompatcache was created by Microsoft to identify application compatibility Issues between 32 bit and 64 bit applications. What does the cache data track?

1 / 1 point

- ( ) File Path
- (•) All of these
- ( ) File Size
- ( ) Last Modified Time
- ( ) None of these

Correct
Appcompatcache was created by Microsoft to identify application compatibility Issues between 32 bit and 64 bit applications. The Cache data tracks file path, size, last modified time, written on shutdown.

52. Information found in the Background Activity Moderator (BAM) sub-key proves?

1 / 1 point

- ( ) Program execution but not by a specific user
- ( ) A change to the file MFT record
- ( ) Nothing
- (•) Program execution by a specific user

Correct
Bam is a service that Controls activity of background applications. This service exists in Windows 10 only after Fall Creators update - version 1709. It is organized by user SID, so it relates back to a specific user and also proves file execution.

53. What do Shellbags track?

1 / 1 point

- ( ) Recently used applications
- (•) Folders or Directories within the windows file system
- ( ) File Times
- ( ) Programs run at startup

Correct
Windows folder view settings (large icons, details, list or even resizing the window itself) and zip files. Proves that the user interacted with that

folder.

54. The _____ hive file stores artifacts such as the Last write time, Install Dates, Application Name, Version, and path to exe or dill

1 / 1 point

- (●) The AmCache Hive File
- ( ) The Sam File
- ( ) The NTUser.dat Hive File
- ( ) The System Hive File

Correct
number of failed logons