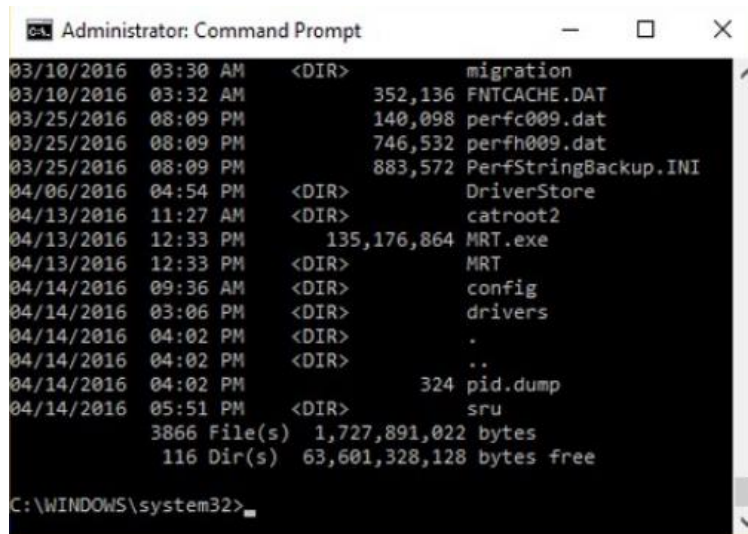


1. Centralized binary logging is a process in which many websites write binary and unformatted log data to a single log file. What extension should the investigator look to find its log file?
 - .cbl
 - .log
 - .txt
 - **.ibl**

2. Gill is a computer forensics investigator who has been called upon to examine a seized computer. This computer, according to the police, was used by a hacker who gained access to numerous banking institutions to steal customer information. After preliminary investigations, Gill finds in the computer's log files that the hacker was able to gain access to these banks through the use of Trojan horses. The hacker then used these Trojan horses to obtain remote access to the companies' domain controllers. From this point, Gill found that the hacker pulled off the SAM files from the domain controllers to then attempt and crack network passwords. What is the most likely password cracking technique used by this hacker to break the user passwords from the SAM files?
 - Brute force attack
 - Syllable attack
 - **Dictionary attack**
 - Hybrid attack

3. NTFS has reduced slack space than FAT, thus having lesser potential to hide data in the slack space. This is because:
 - FAT does not index files
 - FAT is an older and inefficient file system
 - NTFS is a journaling file system
 - **NTFS has lower cluster size space**

4. The given image displays information about date and time of installation of the OS along with service packs, patches, and sub-directories. What command or tool did the investigator use to view this output?



```
Administrator: Command Prompt
03/10/2016 03:30 AM <DIR> migration
03/10/2016 03:32 AM 352,136 FNTCACHE.DAT
03/25/2016 08:09 PM 140,098 perfc009.dat
03/25/2016 08:09 PM 746,532 perfh009.dat
03/25/2016 08:09 PM 883,572 PerfStringBackup.INI
04/06/2016 04:54 PM <DIR> DriverStore
04/13/2016 11:27 AM <DIR> catroot2
04/13/2016 12:33 PM 135,176,864 MRT.exe
04/13/2016 12:33 PM <DIR> MRT
04/14/2016 09:36 AM <DIR> config
04/14/2016 03:06 PM <DIR> drivers
04/14/2016 04:02 PM <DIR> .
04/14/2016 04:02 PM <DIR> ..
04/14/2016 04:02 PM 324 pid.dump
04/14/2016 05:51 PM <DIR> sru
3866 File(s) 1,727,891,022 bytes
116 Dir(s) 63,601,328,128 bytes free
C:\WINDOWS\system32>
```

- dir /o:e
- dir /o:n
- dir /o:s
- **dir /o:d**

5. Which of the following tool can reverse machine code to assembly language?

- Deep Log Analyzer
- PEiD
- **IDA Pro**
- RAM Capturer

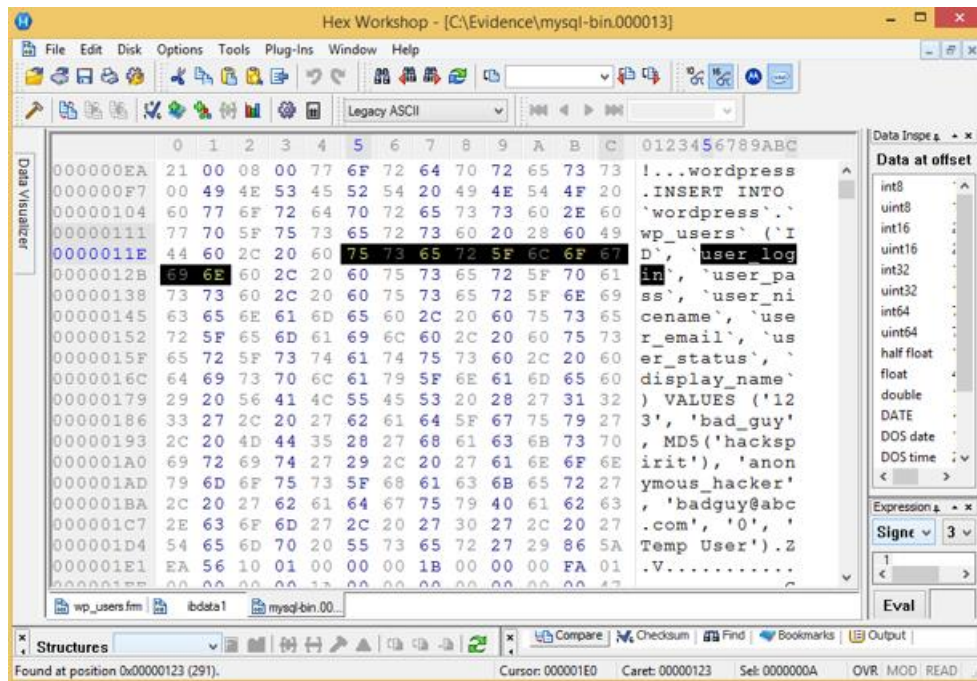
6. Billy, a computer forensics expert, has recovered a large number of DBX files during the forensic investigation of a laptop. Which of the following email clients can he use to analyze the DBX files?

- **Microsoft Outlook Express**
- Mozilla Thunderbird
- Microsoft Outlook
- Eudora

7. When analyzing logs, it is important that the clocks on the devices on the network are synchronized. Which protocol will help in synchronizing these clocks?

- PTP
- **NTP**
- UTC
- Time Protocol

8. NTFS sets a flag for the file once you encrypt it and creates an EFS attribute where it stores Data Decryption Field (DDF) and Data Recovery Field (DOR). Which of the following is not a part of DDF?
- EFS Certificate Hash
 - **Checksum**
 - Encrypted FEK
 - Container Name
9. Analyze the hex representation of mysql-bin.000013 file in the screenshot below. Which of the following will be an inference from this analysis?



- A WordPress user has been created with the username anonymous_hacker
 - A user with username bad_guy has logged into the WordPress web application
 - **A WordPress user has been created with the username bad_guy**
 - An attacker with name anonymous_hacker has re placed a user bad_guy in the WordPress database
10. What malware analysis operation can the investigator perform using the jv16 tool?
- Network Traffic Monitoring/Analysis
 - Files and Folder Monitor
 - **Registry Analysis/Monitoring**
 - Installation Monitor

11. An executive had leaked the company trade secrets through an external drive. What process should the investigation team take if they could retrieve his system?
- Real-Time Analysis
 - Packet Analysis
 - **Postmortem Analysis**
 - Malware Analysis
12. Which command can provide the investigators with details of all the loaded modules on a Linux-based system?
- **lsmod**
 - lsof -m
 - list modules -a
 - plist mod -a
13. If the partition size is 4 GB, each cluster will be 32 K. Even if a file needs only 10 K, the entire 32 K will be allocated, resulting in 22 K of ____
- Cluster space
 - Sector space
 - **Slack space**
 - Deleted space
14. Pick the statement which does not belong to the Rule 804. Hearsay Exceptions; Declarant Unavailable.
- Statement against interest
 - Statement of personal or family history
 - **Statement under belief of impending death**
 - Prior statement by witness
15. Which of the following setups should a tester choose to analyze malware behavior?
- A normal system without internet connect
 - A normal system with internet connection
 - A virtual system with internet connection
 - **A virtual system with network simulation for internet connection**
16. What value of the "Boot Record Signature" is used to indicate that the boot-loader exists?
- AA00
 - **AA55**
 - A100
 - 00AA

17. Which of the following tools is not a data acquisition hardware tool?

- Triage-Responder
- Atola Insight Forensic
- Ultra Kit
- **F-Response Imager**

18. %3cscript%3ealert("XXXXXXXXX")%3c/script%3e is a script obtained from a Cross-Site Scripting attack. What type of encoding has the attacker employed?

- Unicode
- **Hex encoding**
- Double encoding
- Base64

19. Which of the following commands shows you the username and IP address used to access the system via a remote login session and the type of client from which they are accessing the system?

- Net config
- Net stat
- **Net sessions**
- Net share

20. Which of the following file system uses Master File Table (MFT) database to store information about every file and directory on a volume?

- FAT File System
- **NTFS File System**
- ReFS
- exFAT

21. Email archiving is a systematic approach to save and protect the data contained in emails so that it can be accessed fast at a later date. There are two main archive types, namely Local Archive and Server Storage Archive. Which of the following statements is correct while dealing with local archives?

- **It is difficult to deal with the webmail as there is no offline archive in most cases. So consult your counsel on the case as to the best way to approach and gain access to the required data on servers**
- Local archives should be stored together with the server storage archives in order to be admissible in a court of law
- Local archives do not have evidentiary value as the email client may alter the message data

- Server storage archives are the server information and settings stored on a local system, whereas the local archives are the local email client information stored on the mail server

22. What system details can an investigator obtain from the NetBIOS name table cache?

- **List of connections made to other systems**
- List of the system present on a router
- List of files shared between the connected systems
- List of files opened on other systems

23. What do you call the process in which an attacker uses magnetic field over the digital media device to delete any previously stored data?

- **Disk degaussing**
- Disk magnetization
- Disk cleaning
- Disk deletion

24. Which of the following network attacks refers to sending huge volumes of email to an address in an attempt to overflow the mailbox or overwhelm the server where the email address is hosted so as to cause a denial-of-service attack?

- Email spoofing
- **Mail bombing**
- Phishing
- Email spamming

25. Which of the following does Microsoft Exchange E-mail Server use for collaboration of various e-mail applications?

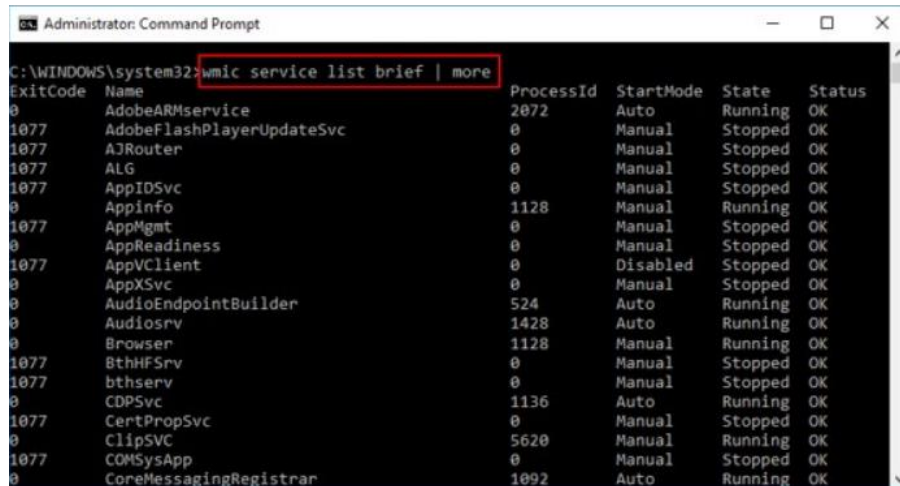
- Internet Message Access Protocol (IMAP)
- **Messaging Application Programming Interface (MAPI)**
- Post Office Protocol version 3 (POP3)
- Simple Mail Transfer Protocol (SMTP)

26. Which of the following tool enables a user to reset his/her lost admin password in a Windows system?

- **Active@ Password Changer**
- SmartKey Password Recovery Bundle Standard
- Advanced Office Password Recovery
- Passware Kit Forensic

27. Which of the following is a database in which information about every file and directory on an NT File System (NTFS) volume is stored?
- **Master File Table**
 - Master Boot Record
 - Volume Boot Record
 - GUID Partition Table
28. As a part of the investigation, Caroline, a forensic expert, was assigned the task to examine the transaction logs pertaining to a database named "Transfers" She used SQL Server Management Studio to collect the active transaction log files of the database. Caroline wants to extract detailed information on the logs, including AllocUnitId, page id, slot id, etc. Which of the following commands does she need to execute in order to extract the desired information?
- DBCC LOG(Transfers, 3)
 - **DBCC LOG(Transfers, 2)**
 - DBCC LOG(Transfers, 1)
 - DBCC LOG(Transfers, 0)
29. Which among the following is an act passed by the U.S. Congress in 2002 to protect investors from the possibility of fraudulent accounting activities by corporations?
- FISMA
 - GLBA
 - **SOX**
 - HIPAA
30. After suspecting a change in MS-Exchange Server storage archive, the investigator has analyzed it. Which of the following components is not an actual part of the archive?
- PRIV.EDB
 - PRIV.STM
 - **PUB.STM**
 - PUB.EDB
31. Chong-lee a forensics executive, suspects that a malware is continuously making copies of files and folders on a victim system to consume the available disk space. What type of test would confirm his claim?
- Dynamic analysis
 - **File fingerprinting**
 - Identifying file obfuscation
 - Static analysis

32. Investigators can use the Type Allocation Code (TAC) to find the model and origin of a mobile device. Where is TAC located in mobile devices?
- **International Mobile Equipment Identifier (IMEI)**
 - International mobile subscriber identity (IMSI)
 - Integrated circuit card identifier (ICCID)
 - Equipment Identity Register (EIR)
33. Charles has accidentally deleted an important file while working on his Mac computer. He wants to recover the deleted file as it contains some of his crucial business secrets. Which of the following tool will help Charles?
- Colasoft's Capsa
 - Xplico
 - Drive Spy
 - **FileSalvage**
34. Which of the following processes is part of the dynamic malware analysis?
- Malware disassembly
 - **Process Monitoring**
 - File fingerprinting
 - Searching for the strings
35. Adam, a forensic analyst, is preparing VMs for analyzing a malware. Which of the following is NOT a best practice?
- Installing malware analysis tools
 - **Enabling shared folders**
 - Using network simulation tools
 - Isolating the host device
36. Which of the following is a device monitoring tool?
- **Driver Detective**
 - RAM Capturer
 - Regs hot
 - Capsa
37. What is the investigator trying to view by issuing the command displayed in the following screenshot?



```
Administrator: Command Prompt
C:\WINDOWS\system32>wmic service list brief | more
ExitCode Name ProcessId StartMode State Status
0 AdobeARMService 2072 Auto Running OK
1077 AdobeFlashPlayerUpdateSvc 0 Manual Stopped OK
1077 AJRouter 0 Manual Stopped OK
1077 ALG 0 Manual Stopped OK
1077 AppIDSvc 0 Manual Stopped OK
0 AppInfo 1128 Manual Running OK
1077 AppMgmt 0 Manual Stopped OK
0 AppReadiness 0 Manual Stopped OK
1077 AppVClient 0 Disabled Stopped OK
0 AppXSvc 0 Manual Stopped OK
0 AudioEndpointBuilder 524 Auto Running OK
0 Audiosrv 1428 Auto Running OK
0 Browser 1128 Manual Running OK
1077 BthHFSrv 0 Manual Stopped OK
1077 bthserv 0 Manual Stopped OK
0 CDPSvc 1136 Auto Running OK
1077 CertPropSvc 0 Manual Stopped OK
0 ClipSVC 5620 Manual Running OK
1077 COMSysApp 0 Manual Stopped OK
0 CoreMessagingRegistrar 1092 Auto Running OK
```

- List of services stopped
- List of services closed recently
- List of services recently started
- **List of services installed**

38. Which of the following tool is used to locate IP addresses?

- Towel root
- **SmartWhois**
- Deep Log Analyzer
- XRY LOGICAL

39. A small law firm located in the Midwest has possibly been breached by a computer hacker who was looking to obtain information on their clientele. The law firm does not have any on-site IT employees but wants to search for evidence of the breach themselves to prevent any possible media attention. Why would this not be recommended?

- Searching could possibly crash the machine or device
- Searching creates cache Files that would hinder the investigation
- **Searching can change date/time stamps**
- Searching for evidence themselves would not have any ill effects

40. One technique for hiding information is to change the file extension from the correct one to the one that might not be noticed by an investigator. For example, changing a .jpg extension to a .doc extension so that a picture file appears to be a document. What can an investigator examine to verify that a file has the correct extension?

- The sector map
- The File Allocation Table
- **The file header**
- The file footer

41. For what purpose do the investigators use tools like iPhoneBrowser, iFunBox, OpenSSHSSH, and iMazing?
- Copying contents of iPhone
 - Debugging iPhone
 - Rooting iPhone
 - **Bypassing iPhone passcode**
42. What technique is used by JPEGs for compression?
- TCD
 - TIFF-8
 - ZIP
 - **DCT**
43. An investigator enters the command `sqlcmd -S WIN-CQQMK62867E -e -s"," -E` as part of collecting the primary data file and logs from a database. What does the "WIN-CQQMK62867E" represent?
- Operating system of the system
 - Network credentials of the database
 - **Name of SQL Server**
 - Name of the Database
44. During forensics investigations, investigators tend to first collect the system time and then compare it with UTC. What does the abbreviation UTC stand for?
- Universal Computer Time
 - **Coordinated Universal Time**
 - Universal Time for Computers
 - Correlated Universal Time
45. Which of the following commands shows you all of the network services running on Windows-based servers?
- **Net start**
 - Net config
 - Net Session
 - Net use
46. Depending upon the jurisdictional areas, different laws apply to different incidents. Which of the following law is related to fraud and related activity in connection with computers?
- 18 USC §1371

- 18 USC §1029
- **18 USC §1030**
- 18 USC §1361

47. Which of the following is a federal law enacted in the US to control the ways that financial institutions deal with the private information of individuals?

- PCI DSS
- SOX
- HIPAA 1996
- **GLBA**

48. What is an investigator looking for in the rp.log file stored in a system running on Windows 10 operating system?

- Restore point interval
- Restore point functions
- Automatically created restore points
- **System CheckPoints required for restoring**

49. Andie, a network administrator, suspects unusual network services running on a Windows system. Which of the following commands should he use to verify unusual network services started on a Windows system?

- net serv
- lusrmgr
- netmgr
- **net start**

50. Jvanovich, a forensics investigator, is trying to extract complete information about running processes from a system. Where should he look apart from the RAM and virtual memory?

- **Swap space**
- Files and documents
- Application data
- Slack space

51. Which of the following is NOT a part of pre-investigation phase?

- Gathering information about the incident
- Creating an investigation team
- Building forensics workstation
- **Gathering evidence data**

52. UEFI is a specification that defines a software interface between an OS and platform firmware. Where does this interface store information about files present on a disk?

- Master Boot Record (MBR)
- BIOS-MBR
- BIOS Parameter Block
- **GUID Partition Table (GPT)**

53. An investigator is analyzing a checkpoint firewall log and comes across symbols. What type of log is he looking at?



- **An email marked as potential spam**
- Malicious URL detected
- Connection rejected
- Security event was monitored but not stopped

54. A suspect is accused of violating the acceptable use of computing resources as he has visited adult websites and downloaded images. The investigator wants to demonstrate that the suspect did indeed visit these sites. However, the suspect has cleared the search history and emptied the cookie cache. Moreover, he has removed any images he might have downloaded. What can the investigator do to prove the violation? Choose the most feasible option.

- Approach the websites for evidence
- **Image the disk and try to recover deleted files**
- Check the Windows registry for connection data (You may or may not recover)
- Seek the help of co-workers who are eye-witnesses

55. During an investigation, Noel found the following SIM card from the suspect's mobile. What does the code 89 44 represent?



- TAC and Industry Identifier
- **Industry Identifier and Country code**
- Individual Account Identification Number and Country Code
- Issuer Identifier Number and TAC

56. Which rule requires an original recording to be provided to prove the content of a recording?

- **1002**
- 1004
- 1003
- 1005

57. Lynne receives the following email:

Dear lynne@gmail.com!

We are sorry to inform you that your ID has been temporarily frozen due to incorrect or missing information saved at 2016/11 /1 O 20:40:24 You have 24 hours to fix this problem or risk to be closed permanently!

To proceed Please Connect>> My Apple ID

Thank You

The link to My Apple ID shows <http://byggarbetsplatsen.se/backup/signon/>

What type of attack is this?

- Email Spamming
- Mail Bombing
- **Phishing**
- Email Spoofing

58. Which of the following files stores information about a local Google Drive installation such as User email ID, Local Sync Root Path, and Client version installed?

- config.db
- sigstore.db
- **Sync_config.db**
- filecache.db

59. Which part of Metasploit framework helps users to hide the data related to a previously deleted file or currently unused by the allocated file.

- **Slacker**
- Waffin FS
- FragFS
- RuneFS

60. In which registry does the system store the Microsoft security IDs?

- **HKEY_LOCAL_MACHINE (HKLM)**
- HKEY_CLASSES_ROOT (HKCR)

- HKEY_CURRENT_USER (HKCU)
- HKEY_CURRENT_CONFIG (HKCC)

61. Which one of the following is not a first response procedure?

- Fill forms
- **Crack passwords**
- Preserve volatile data
- Take photos

62. Identify the file system that uses \$Bitmap file to keep track of all used and unused clusters on a volume.

- EXT
- **NTFS**
- FAT
- FAT32

63. Jacob is a computer forensics investigator with over 10 years of experience in investigations and has written over 50 articles on computer forensics. He has been called upon as a qualified witness to testify the accuracy and integrity of the technical log files gathered in an investigation into computer fraud. What is the term used for Jacob's testimony in this case?

- Reiteration
- Certification
- **Authentication**
- Justification

64. Which of the following tool creates a bit-by-bit image of an evidence media?

- Recuva
- FileMerlin
- **AccessData FTK Imager**
- Xplico

65. Which of the following tool enables data acquisition and duplication?

- Colasoft's Capsa
- **Drive Spy**
- Wireshark
- Xplico

66. During the trial, an investigator observes that one of the principal witnesses is severely ill and cannot be present for the hearing. He decides to record the evidence and present it to the court. Under which rule should he present such evidence?

- **Limited admissibility**
- Rule 1003: Admissibility of Duplicates
- Locard's Principle
- Hearsay

67. Which of the following is a non-zero data that an application allocates on a hard disk cluster in systems running on Windows OS?

- Meta Block Group
- Slack Space
- **Master File Table**
- Sparse File

68. An International Mobile Equipment Identifier (IMEI) is a 15-digit number that indicates the manufacturer, model type, and country of approval for GSM devices. The first eight digits of an IMEI number that provide information about the model and origin of the mobile device are also known as:

- Manufacturer Identification Code (MIC)
- Integrated Circuit Code (ICC)
- Device Origin Code (DOC)
- **Type Allocation Code (TAC)**

69. What does the 56.58.152.114(445) denote in a Cisco router log?

Jun 19 23:25:46.125 EST: o/oSEC-4-IPACCESSLOGP: list internet-inbound denied UDP 67.124.115.35(8084) -> 56.58.152.114(445). 1 packet

- None of the above
- Source IP address
- Login IP address
- **Destination IP address**

70. Which principle states that "anyone or anything, entering a crime scene takes something of the scene with them, and leaves something of themselves behind when they leave"?

- Enterprise Theory of Investigation
- Evidence Theory of Investigation
- Locard's Evidence Principle
- **Locard's Exchange Principle**

71. Which of the following Event Correlation Approach checks and compares all the fields systematically and intentionally for positive and negative correlation with each other to determine the correlation across one or multiple fields?

- **Automated Field Correlation**
- Rule-Based Approach
- Field-Based Approach
- Graph-Based Approach

72. Which of the following is a responsibility of the first responder?

- **Collect as much information about the incident as possible**
- Determine the severity of the incident
- Document the findings
- Share the collected information to determine the root cause

73. Which layer of iOS architecture should a forensics investigator evaluate to analyze services such as Threading, File Access, Preferences, Networking and high-level features?

- Cocoa Touch
- **Core OS**
- Media services
- Core Services

74. During an investigation of an XSS attack, the investigator comes across the term "[a-zA-Z0-9\%]%" in analyzed evidence details. What is the expression used for?

- Checks for opening angle bracket, its hex or double-encoded hex equivalent
- Checks for closing angle bracket, hex or double-encoded hex equivalent
- **Checks for forward slash used in HTML closing tags, its hex or double-encoded hex equivalent**
- Checks for upper and lower-case alphanumeric string inside the tag, or its hex representation

75. Stephen is checking an image using Compare Files by The Wizard, and he sees the file signature is shown as FF D8 FF E1. What is the file type of the image?

- png
- gif
- bmp
- **Jpeg**

76. What is the investigator trying to view by issuing the command displayed in the following screenshot?

- List of services stopped

- List of services closed recently
- List of services recently started
- **List of services installed**

77. An attacker has compromised a cloud environment of a company and used the employee information to perform an identity theft attack. Which type of attack is this?

- Cloud as a service
- Cloud as a tool
- **Cloud as a subject**
- Cloud as an object

78. Which of the following data structures stores attributes of a process, as well as pointers to other attributes and data structures?

- **EProcess**
- Dun1pChk
- Registry
- Lsproc

79. Which of the following is a precomputed table containing word lists like dictionary files and brute force lists and their hash values?

- Master file Table (MFT)
- **Rainbow Table**
- Directory Table
- Partition Table

80. Which list contains the most recent actions performed by a Windows User?

- Windows Error Log
- **MRU**
- Recents
- Activity

81. Files stored in the Recycle Bin in its physical location are renamed as Dxy.ext, where "x" represents the _____

- Original file name's extension
- Sequential number
- Original file name
- **Drive name**

82. Gary is checking for the devices connected to USB ports of a suspect system during an investigation. Select the appropriate tool that will help him document all the connected devices.

- **Devcon**
- Reg.exe
- DevScan
- fsutil

83. The Apache server saves diagnostic information and error messages that it encounters while processing requests. The default path of this file is `usr/local/apache/logs/error.log` in Linux. Identify the Apache error log from the following logs.

- 127.0.0.1 - frank [10/Oct/2000:13:55:36 -0700]"GET /apache_pb.gif HTTP/ 1.0" 200 2326
- [Wed Oct 11 14:32:52 2000] [error] [client 127.0.0.1] client denied by server configuration: /export/home/live/ap/htdocs/test
- http://victim.com/scripts/../../../../af../../../../af../../../../af../../../../af../../../../winnt/system32/cmd.exe?/c+dir+C:\Winnt\system32\Logfiles\W3SVC1
- 127.0.0.1 - - [10/Apr/2007:10:39:11 +0300] [error] "GET /apache_pb.gif HTTP/ 1.0" 200 2326

84. Examination of a computer by a technically unauthorized person will almost always result in

- Completely accurate results of the examination
- The chain of custody being fully maintained
- **Rendering any evidence found inadmissible in a court of law**
- Rendering any evidence found admissible in a court of law

85. When a user deletes a file or folder, the system stores complete path including the original filename in a special hidden file called "INF02" in the Recycled folder. If the INF02 file is deleted, it is recovered when you _____

- Download the file from Microsoft website
- Undo the last action performed on the system
- **Reboot Windows**
- Use a recovery tool to undelete the file

86. What is the purpose of using Obfuscator in malware?

- **Avoid detection by security mechanisms**
- Execute malicious code in the system
- Avoid encryption while passing through a VPN
- Propagate malware to other connected devices

87. Casey has acquired data from a hard disk in an open source acquisition format that allows her to generate compressed or uncompressed image files. What format did she use?

- **Advanced Forensics Format (AFF)**
- Raw Format
- Proprietary Format
- Portable Document Format

88. Which among the following search warrants allows the first responder to search and seize the victim's computer components such as hardware, software, storage devices, and documentation?

- Service Provider Search Warrant
- John Doe Search Warrant
- Citizen Informant Search Warrant
- **Electronic Storage Device Search Warrant**

89. In a Linux-based system, what does the command "Last -F" display?

- Recently opened files
- **Login and logout times and dates of the system**
- Last functions performed
- Last run processes

90. What does the command "C:\>wevtutil gl <log name>" display?

- List of available Event Logs
- **Configuration information of a specific Event Log**
- Event logs are saved in .xml format
- Event log record structure

91. Which of the following is a list of recently used programs or opened files?

- Master File Table (MFT)
- **Most Recently Used (MRU)**
- Recently Used Programs (RUP)
- GUID Partition Table (GPT)

92. Which of the following commands shows you the names of all open shared files on a server and the number of file locks on each file?

- Net config
- Net sessions
- **Net file**
- Net share

93. Which of the following ISO standard defines file systems and protocol for exchanging data between optical disks?
- IEC 3490
 - **ISO 9660**
 - ISO/IEC 13940
 - ISO 9060
94. Adam, a forensic investigator, is investigating an attack on Microsoft Exchange Server of a large organization. As the first step of the investigation, he examined the PRIV.EDB file and found the source from where the mail originated and the name of the file that disappeared upon execution. Now, he wants to examine the MIME stream content. Which of the following files is he going to examine?
- PRIV.EDB
 - PUB.EDB
 - **PRIV.STM**
 - gwcheck.db
95. Jason discovered a file named \$RIYG6VR.doc in the C:\\$Recycle.Bin\<USER SID>\ while analyzing a hard disk image for the deleted data. What inferences can he make from the file name?
- **It is a deleted doc file**
 - It is a doc file deleted in seventh sequential order
 - RIYG6VR.doc is the name of the doc file deleted from the system
 - It is file deleted from R drive
96. Which of the following Registry components include offsets to other cells as well as the LastWrite time for the key?
- Value list cell
 - Security descriptor cell
 - **Key cell**
 - Value cell
97. Which of the following Windows-based tool displays who is logged onto a computer, either locally or remotely?
- **PSLoggedon**
 - Process Monitor
 - TCPView
 - Tokenmon

98. Where should the investigator look for the Edge browser's browsing records, including history, cache, and cookies?
- Sparse files
 - Slack Space
 - Virtual Memory
 - **ESE Database**
99. Which of the following files stores information about local Dropbox installation and account, email IDs linked with the account, current version/build for the local application, the host_id, and local path information?
- **config.db**
 - sigstore.db
 - host.db
 - filecache.db
100. What is the framework used for application development for iOS-based mobile devices?
- **Cocoa Touch**
 - Zygote
 - AirPlay
 - Dalvik
101. Which of the following file formats allows the user to compress the acquired data as well as keep it randomly accessible?
- Advanced Forensics Format (AFF)
 - **Generic Forensic Zip (gfzip)**
 - Advanced Forensic Framework 4
 - Proprietary Format
102. Rusty, a computer forensics apprentice, uses the command nbtstat -c while analyzing the network information in a suspect system. What information is he looking for?
- **Contents of the NetBIOS name cache**
 - Contents of the network routing table
 - Network connections
 - Status of the network carrier
103. Event correlation is the process of finding relevance between the events that produce a final result. What type of correlation will help an organization to correlate events across a set of servers, systems, routers and network?
- Multiple-platform correlation
 - **Cross-platform correlation**

- Network-platform correlation
- Same-platform correlation

104. You are working as an independent computer forensics investigator and received a call from a systems administrator for a local school system requesting your assistance. One of the students at the local high school is suspected of downloading inappropriate images from the Internet to a PC in the Computer Lab. When you arrive at the school, the systems administrator hands you a hard drive and tells you that he made a "simple backup copy" of the hard drive in the PC and put it on this drive and requests that you examine the drive for evidence of the suspected images. You inform him that a "simple backup copy" will not provide deleted files or recover file fragments. What type of copy do you need to make to ensure that the evidence found is complete and admissible in future proceeding?

- Robust copy
- Incremental backup copy
- Full backup copy
- **Bit-stream copy**

105. Which of the following is an iOS Jailbreaking tool?

- **Redsn0w**
- Towel root
- Kingo Android ROOT
- One Click Root

106. Which of the following is a tool to reset Windows admin password?

- TestDisk for Windows
- Windows Data Recovery Software
- **Windows Password Recovery Bootdisk**
- R-Studio

107. What is the name of the first reserved sector in File allocation table?

- BIOS Parameter Block
- Partition Boot Sector
- Volume Boot Record
- **Master Boot Record**

108. Which file is a sequence of bytes organized into blocks understandable by the system's linker?

- None of these
- source file
- **Object file**

- executable file

109. An expert witness is a _____ who is normally appointed by a party to assist in the formulation and preparation of a party's claim or defense.

- Witness present at the crime scene
- **Subject matter specialist**
- Expert in criminal investigation
- Expert law graduate appointed by attorney

110. Joshua is analyzing an MSSQL database for finding the attack evidence and other details, where should he look for the database logs?

- Model.log
- Model.lgf
- Model.txt
- **Model.ldf**

111. Which network attack is described by the following statement? "At least five Russian major banks came under a continuous hacker attack, although online client services were not disrupted. The attack came from a wide-scale botnet involving at least 24,000 computers, located in 30 countries."

- Sniffer Attack
- Man-in-the-Middle Attack
- Buffer Overflow
- **DDoS**

112. Amelia has got an email from a well-reputed company stating in the subject line that she has won a prize money, whereas the email body says that she has to pay a certain amount for being eligible for the contest. Which of the following acts does the email breach?

- **CAN-SPAM Act**
- GLBA
- HIPAA
- SOX

113. What is the capacity of Recycle bin in a system running on Windows Vista?

- 10% of the partition space
- **Unlimited**
- 3.99GB
- 2.99GB

114. Hard disk data addressing is a method of allotting addresses to each ___ of data on a hard disk.
- Operating system block
 - **Physical block**
 - Logical block
 - Hard disk block
115. In which implementation of RAID will the image of a Hardware RAID volume be different from the image taken separately from the disks?
- **It will always be different**
 - RAID 1
 - The images will always be identical because data is mirrored for redundancy
 - RAID 0
116. Which of the following technique creates a replica of an evidence media?
- Data Extraction
 - Backup
 - **Bit Stream Imaging**
 - Data Deduplication
117. Which of the following attacks allows an attacker to access restricted directories, including application source code, configuration and critical system files, and execute commands outside of the web server's root directory?
- Unvalidated input
 - Security misconfiguration
 - Parameter/form tampering
 - **Directory traversal**
118. An investigator has extracted the device descriptor for a 1 GB thumb drive that looks like: Disk&Ven_Best_Buy&Prod_Geek_Squad_U3&Rev 6.15. What does the "Geek_Squad" part represent?
- Developer description
 - **Product description**
 - Software or OS used
 - Manufacturer Details
119. Sniffers that place NICs in promiscuous mode work at what layer of the OSI model?
- **Physical**
 - Transport
 - Network

- Session

120. Which of the following techniques can be used to beat steganography?

- Decryption
- Cryptanalysis
- **Steganalysis**
- Encryption

121. Which among the following U.S. laws requires financial institutions/companies that offer consumers financial products or services such as loans, financial or investment advice, or insurance to protect their customers' information against security threats?

- HIPAA
- FISMA
- **GLBA**
- SOX

122. Which of the following tasks DOES NOT come under the investigation phase of a cybercrime forensics investigation case?

- Data analysis
- Data collection
- Secure the evidence
- **First response**

123. What is the investigator trying to analyze if the system gives the following image as output?

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32\C:\Users\Admin\Desktop\logonSessions\logonsessions.exe

Logonsessions v1.3
Copyright (C) 2004-2015 Mark Russinovich
Sysinternals - www.sysinternals.com

[0] Logon session 00000000:000003e7:
  User name:      WORKGROUP\RD-006$
  Auth package:   NTLM
  Logon type:     (none)
  Session:        0
  Sid:            5-1-5-18
  Logon time:     3/10/2016 3:32:46 AM
  Logon server:
  DNS Domain:
  UPN:

[1] Logon session 00000000:00009209:
  User name:
  Auth package:   NTLM
  Logon type:     (none)
  Session:        0
  Sid:            (none)
  Logon time:     3/10/2016 3:32:46 AM
  Logon server:
  DNS Domain:
  UPN:

[2] Logon session 00000000:000003e4:
  User name:      WORKGROUP\RD-006$
  Auth package:   Negotiate
  Logon type:     Service
  Session:        0
  Sid:            5-1-5-20
  Logon time:     3/10/2016 3:32:46 AM
  Logon server:
  DNS Domain:
  UPN:
```

- All the logon sessions
- Details of users who can logon
- **Currently active logon sessions**
- Inactive logon sessions

124. Ron, a computer forensics expert, is investigating a case involving corporate espionage. He has recovered several mobile computing devices from the crime scene. One of the evidence that Ron possesses is a mobile phone from Nokia that was left in ON condition. Ron needs to recover the IMEI number of the device to establish the identity of the device owner. Which of the following key combinations can he use to recover the IMEI number?

- #06#
- *#06#
- **#*06*#**
- *IMEI#

125. Richard is extracting volatile data from a system and uses the command `doskey /history`. What is he trying to extract?
- Passwords used across the system
 - History of the browser
 - **Previously typed commands**
 - Events history
126. Microsoft Security IDs are available in Windows Registry Editor. The path to locate IDs in Windows 7 is:
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Profilelist
 - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Regedit
 - **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList**
 - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Reglist
127. Which of the following attack uses HTML tags like `<script></script>`?
- Phishing
 - SQL injection
 - **XSS attack**
 - Spam
128. While analyzing a hard disk, the investigator finds that the file system does not use UEFI-based interface. Which of the following operating systems is present on the hard disk?
- Windows 10
 - **Windows 7**
 - Windows 8.1
 - Windows 8
129. The surface of a hard disk consists of several concentric rings known as tracks; each of these tracks has smaller partitions called disk blocks. What is the size of each block?
- 256 bits
 - 256 bytes
 - **512 bytes**
 - 512 bits
130. Which of the following protocols allows non-ASCII files, such as video, graphics, and audio, to be sent through the email messages?
- BINHEX

- UT-16
- **MIME**
- UUCODE

131. When a user deletes a file, the system creates a \$I file to store its details. What detail does the \$I file not contain?

- File Name
- Time and date of deletion
- **File origin and modification**
- File Size

132. Graphics Interchange Format (GIF) is a _____ RGB bitmap image format for images with up to 256 distinct colors per frame.

- 32-bit
- **8-bit**
- 16-bit
- 24-bit

133. Which password cracking technique uses details such as length of the password, character sets used to construct the password, etc.?

- **Rule-based attack**
- Brute force attack
- Man in the middle attack
- Dictionary attack

134. CAN-SPAM Act requires that you:

- Don't tell the recipients where you are located
- Don't identify the message as an ad
- **Don't use deceptive subject lines**
- Don't use true header information

135. Which of the following Perl scripts will help an investigator to access the executable image of a process?

- Lpsi.pl
- **Lspi.pl**
- Lspd.pl
- Lspm.pl

136. Which MySQL log file contains information on server start and stop?

- Slow query log file
- General query log file
- **Error log file**
- Binary log

137. Which of the following application password cracking tool can discover all password-protected items on a computer and decrypts them?

- **Passware Kit Forensic**
- TestDisk for Windows
- Windows Password Recovery Bootdisk
- R-Studio

138. Select the data that a virtual memory would store in a Windows-based system.

- Information or metadata of the files
- Application data
- **Running processes**
- Documents and other files

139. Madison is on trial for allegedly breaking into her university's internal network. The police raided her dorm room and seized all of her computer equipment. Madison's lawyer is trying to convince the judge that the seizure was unfounded and baseless. Under which US Amendment is Madison's lawyer trying to prove the police violated?

- The 10th Amendment
- The 5th Amendment
- **The 4th Amendment**
- The 1st Amendment

140. Which of the following techniques delete the files permanently?

- Steganography
- Trail obfuscation
- Data Hiding
- **Artifact Wiping**

141. You have been asked to investigate the possibility of computer fraud in the finance department of a company. It is suspected that a staff member has been committing finance fraud by printing cheques that have not been authorized. You have exhaustively searched all data files on a bitmap image of the target computer but have found no evidence. You suspect the files may not have been saved. What should you examine next in this case?

- **The swap file**
- The metadata

- The registry
- The recycle bin

142. Which of the following examinations refers to the process of providing the opposing side on a trial the opportunity to question a witness?

- Witness Examination
- **Cross Examination**
- Direct Examination
- Indirect Examination

143. What is cold boot (hard boot)?

- It is the process of restarting a computer that is already in sleep mode
- It is the process of restarting a computer that is already turned on through the operating system
- It is the process of shutting down a computer from a powered-on or on state
- **It is the process of starting a computer from a powered-down or off state**

144. In Steganalysis, which of the following describes a Known-stego attack?

- **Original and stego-object are available and the steganography algorithm is known**
- The hidden message and the corresponding stego-image are known
- During the communication process, active attackers can change cover
- Only the steganography medium is available for analysis

145. Which of the following email headers specifies an address for mailer-generated errors, like "no such user" bounce messages (instead of the sender's address)?

- Content-Transfer-Encoding header
- Mime-Version header
- **Errors-To header**
- Content-Type header

146. A Linux system is undergoing investigation. In which directory should the investigators look for its current state data if the system is in powered on state?

- /auth
- /var/spool/cron/
- **/proc**
- /var/log/debug

147. Which of the following does not describe the type of data density on a hard disk?

- Track density

- **Volume density**
- Linear or recording density
- Areal density

148. Brian needs to acquire data from RAID storage. Which of the following acquisition methods is recommended to retrieve only the data relevant to the investigation?

- Bit-by-bit Acquisition
- Static Acquisition
- Bit-stream disk-to-disk Acquisition
- **Sparse or Logical Acquisition**