1.	**What artifact is available in the file system when the Firefox browser is placed into private browsing mode?**	Downloaded file(s)
2.	**Which Security Event Category is marked in an event log entry when a user account logs off a system?**	Logon Events
3.	**What is the main metada artifact in IE version 6-9?**	Index.dat
4.	**Under the registry key shown below, the last drive letter can be found for which of the following device types?**	MSC
5.	**An investigation involves a Windows user who is alleged to have violated Internet-use policy. The user uninstalled Firefox in order to hide their activity. Which approach can recover browser artifacts?**	Analyze places.sqlite
6.	**You are looking for webmail remnants on a system image. The person who captured the original image assures you that the subject being investigated did not have Private Mode turned on, nor did they have time to clear the cache before image was captured. You should be able to see something relating to webmail, but string searches find nothing. Which of the following is the most plausible explanation?**	The webmail session was sent over in a compressed format, expand to reveal original HTML messages.
7.	**Which of the following is a reason to profile a user when investigating a Windows system?**	To determine the security identifier (SID) so evidence artifacts can be correlated to a user.
8.	**What value should be set in the KAPE target file for the VSS output to maintain the folder structure of the scanned drive?**	Recreate Directories
9.		SYSTEM\CurrentCon-

	Where would the following registry key be found? Disk&Ven_Kinston&Prod_DataTraveler_SE9&Rev_PMAP	trolSet\Enum\USBTOR
10.	**Examin the image of a Firefox Cache item below. What is being identified in the box? Server:ngix**	The browser HTTP header for the image file
11.	**What part of a LNK file reveals the shell path to the target file?**	PIDL
12.	**Which of the following is an example of non-violatile data?**	Executable files on a system
13.	**When examining Event Logs for a computer, you see an event that states that the Event Log Service was started. What sort of Event is this?**	Information
14.	**Memory analysis shows that cleaner software was running on a host but the host user claims that they have no knowledge of the application running. They claim that the cleaner software must have been running in the background.**	NTUSER.DAT\Softwar
15.	**Examine the below, what does the presence of the file memory.dmp indicate to a forensic examiner?**	Full copy of the memory just prior to the workstation last crashing
16.	**Which of the following statements is supported by the image below?**	The file was last opened at 8:04:38 PM on 10/21/2013
17.	**What artifact will be found in the directory in the image below?**	Web storage data
18.	**Review the email header shown below and determine what key information is missing? Subject: A better way to pollinate your farm today.**	The "Message-ID:" value

19.	**Which file should an analyst search for the email login used to authenticate to box servers?**	metrics.db
20.	**Analyze the image below. Which conclusion can be drawn from facts?**	chrome.exe was first run in September of 2009
21.	**You are examining an image of a Windows XP system, focusing on a direntory containing photos from a digital camera. Some photos appear to be missing and you suspect that the computer had been scrubbed with a file shredding tool in order to hide evidence.**	Search for all instances of "thumb.db." The files may contain thumbnails of images that have since been deleted or moved.
22.	**You are examining the image of a desktop system and have located a file names "Totally Not Bad Stuff" on the custodians drive.**	Volatile memory acquisition
23.	**Which operating system is most likely to contain the folder shown in the attached screen capture?**	Windows 7
24.	**What Security Event Category would be used to mark an event that tracked the shutting down of a system?**	System Events
25.	**During an investigation a user is asked if they had ever accessed the folder C:\temp\xpf\malware on their workstation**	Shellbags
26.	**Which of the following is an example of volatile data?**	Open files
27.	**A user is suspected of accessing websites that are not approved by the corporate security policy. However, a review of the Mozilla Firefox history file for the user does not indicate any inappropriate site visits.**	Missing record indexes in the history file
28.	**Which artifact contains the HTTP header used to download the file?**	Firefox Cache2 entries

29.	**Which of the following occurs to the space in the Windows Registry when a key is deleted?**	Unallocated and freed up for new data
30.	**What technique is normally used to identify chat messages?**	Data stream carving
31.	**Where are the local files synchronized by the Google Workspace (G Suite) File Stream application stored?**	A folder called "My Drive" in a virtual volume mounted on the user's system.
32.	**Which of the following types of information can be found in the Firefox cache?**	The HTTP header from a visited website
33.	**What does the web notes feature in Microsoft's Edge browser allow a user to perform?**	Annotate and save a local copy of a webpage
34.	**Review the image below of a memory acquisition. Which of the following is a breach of forensic methodology? AccessData FTK Imager 3.1.1.8**	The image is being written to the local drive
35.	**You are investigating the compromise of a workstation that contains sensitive information. During the course of the examination you discover the following entry in the security logs.**	Via Remote Desktop
36.	**Examining the image below. Which values will be written to the black section of the image for the file on a Windows NTFS system?**	x00
37.	**The log data below is a compressed Windows event from a compromised workstation. Which of the following statements describes the activity surrounding the file AA_V3(1).EXE?**	The files were executed from separate directories
38.		

	You are examining an image of a Windows system. In the C:\Windows\Prefetch directory you find an entry for "EVILBIN.EXE" Assuming the file was legitimately created by the operating system, what does this file's existence mean to you, as the forensic investigator?	EVILBIN.EXE has been run at least once on this system
39.	**You are responding to an incident in progress on a workstation. Why is it important to check for the presence of encryption on the suspect workstation before turning it off?**	Data on mounted volumes and decryption keys stored as volatile data may be lost
40.	**What has the analyst identified in the box in the image below?**	Device serial number
41.	**Where is the image displayed on the right of the application Thumbs Viewer located?**	In the Thumbs.db database file
42.	**What can be concluded using the following registry data from a Windows 10 host?**	BrokerInfrastructure is a service that will start at boot
43.	**You are investigating a forensic image of a Windows 7 machine shared by multiple user accounts. You are using a computer program to view thumbcache files in C:\Users\harley\AppData\Local\Microsoft\Windows\Explorer.**	The directory C:\Share\Photos was opened in Explorer by user "harley"
44.	**Which user action will create an entry in the folder C:\Users\<Users>\AppData\Local\Temp\WPDNSE**	Opening a file from a USB key on a Windows 8 host
45.	**Which registry hive will contain ShellBags information**	UsrClass
46.	**You run across the following message when performing email forensics, Which of the following statements is correct?**	This message has been encrypted with an end to end encryption proto-

		col; the local copy remains encrypted.
47.	**What command line will be generated from the KAPE options selected in the image?**	.\-kape.exe--tsource E:\Users\Donald--tdest G:\Doanld_Blake_Evic
48.	**Which Windows Event Log records details about every device connection?**	Partition/Diagnostic
49.	**An analyst has captured memory from a target host and uses EDD to determine that the drive is encrypted. Which option will acquire the disk in an unencrypted state?**	Image the logical drive
50.	**A 768 byte file is written to a drive that uses NTFS with 2048 clusters with 1024 sectors. What term is used to describe the 2nd sector which is not written to by the 768 byte file in the cluster?**	Slack space
51.	**Which of the following is metada?**	Cryptographic hash of a binary file
52.	**For a live system, when should logical imaging be used instead of physical imaging?**	When the hard drive is encrypted
53.	**Examine the image below. Which of the following statements is supported by the artifact 9b9cdc69c1c24e2b.automaticDestinations-ms?**	The application Notepad was launched at some point on the workstation
54.	**The information shown below is found in which Windows registry hive?**	SAM
55.		

	Which of the following artifacts is created by a user browsing to a folder containing images on their Windows 10 system by issuing the command \\localhost\c$\temp?	A thumbs.db entry for each image in the folder
56.	**An analyst wants to verify the state of the information captured by the System Resource Usage Monitor. Which of the following would she use to run the esentutl tool?**	C:\Windows\System32\sru\SRUDB.dat
57.	**From the screenshot of actual email reader excerpts, assuming the contents have not been altered, which of the following is the accurate source address?**	66.148.116.54
58.	**Where can the event logs for the Microsoft Windows 7 operating system be found?**	%system-root%System32\winevt\logs
59.	**How should an analyst identify deleted JPEG files that are able to be carved from an E01 image?**	The header of the file type
60.	**Which registry hive contains the date and time a USB key was first connected to a computer?**	System
61.	**Which Firefox browser file contains the setting for clearing session history?**	prefs.js
62.	**Where should an examiner look to recover folders and files that may have been deleted and overwritten on a Windows 7+ system?**	Volume Shadow Copies
63.	**Which of the following allows Windows to alert the user that this file has been downloaded from the internet? Do you want to allow this app to make changes to your device? (Wireshark)**	Alternate data streams?
64.	**Analyze the provided screenshot. Which history file is likely synced?**	B-13024440806774
65.		

	Which of the following dates, from the SYSTEM hive, will match what is found in Windows tool systeminfo?	InstallTIme>Data Interprter>Windos FILETIME 2017-02-03
66.	**At the Data Layer, which of the following defines unallocated or free space?**	Data blocks that are not being used by a file
67.	**Given the following registry data, which value was added most recently?**	0
68.	**What artifact can inform an examiner that a specific user, on a multi-user Windows 10 computer, executes Chrome from a desktop shortcut, whereas other users on the host execute Chrome from the taskbar?**	UserAssist Key
69.	**Which of the following steps could an attacker without administrative privileges take to cover their attempted logon activity on a Windows host?**	Flood the log with trivial events
70.	**Which Windows 10 folder is highlighted in the following image of the registry? (BagMRU)**	Desktop
71.	**You are asked to investigate reports of inappropriate internet usage originating from a suspect workstation. Which registry hive will contain the url if the user copied and pasted the address into internet explorer?**	NTUSER
72.	**An engineer examining an image of Windows 10 system suspects that digital photos were deleted. The unallocated space of the image drive consists entirely of zeros indicating a file shredding tool was used. Which of the following options could find parts of the missing photos ?**	Search for filename thumbcache_*.db as these contain thumbnails for all images that were viewed on the system
73.	**What information is recorded in Internet Explorer's history files?**	

		Local and remote (via network shares) file access
74.	**These email headers, which statement describes the reliability of the message? Received: from mail.giac.org (smtpgw.giac.org.)**	This message appears to be legitimate. The originating MTA appears to match the sender domain.