Possible Test Questions Digital Forensics WS 2022

Question 1

In the RAM of a computer, you can find plenty of valuable information for investigations that are never written to disk, and are lost once the PC is shut down.

1. Describe in your own words how the cold boot attack works.
    - A cold boot attack is a side channel attack on the RAM of a computer. A memory dump is made after the computer is turned off by booting it again with a minimal OS which does not need much RAM.
2. What information can you retrieve from RAM? Name at least six different artifacts.
    - Running processes
    - Information about executable files
    - Registry keys
    - Information about network activity
    - User logins
    - Passwords and cryptographic keys
    - Malware

Question 2

NTFS is one of the most common file system for computers.

1. Describe in your own words how the Master File Table in NTFS is structured.
    - The Master File Table (MFT) is a index structure that stores everything regarding files, directories and metadata of those. Each entry has a fixed size of usually 1K.
    - One MFT entry has a header with n attributes
    - Unique ID (48bit), starting with o + 16bit sequence number = 64bit File Reference Address for each file and directory
    - First 16 entries are reserved for file system metadata
    - MFT entry attributes (at least):
        - $STANDARD INFORMATION
        - $FILE NAME
        - $INDEX ROOT (for directories)
        - $DATA (for files)
2. What happens on disk when a file is deleted (without it going to the recycle bin)? What methods do you know that can be used to still retrieve the file content?
    - The file name has it's first letter changed to a sigma, and then the location of the stored file is considered unallocated (may now be overwritten)
    - To find the deleted files for a specific parent directory, the MFT entry of the directory is determined and the MFT is scanned to find all unallocated entries that reference that directory as its parent directory. The file name is stored in the MFT entry so the full path can be determined using the path of the parent directory and the name stored in the file's MFT entry.

3. You are looking for a file with a specific known string (something distinct, like "AAAAAAAAAAAAAAAAAAAAAAAAAA") in it. How can you a) identify and b) retrieve all files that contain that string?
    - Recursive pattern matching (grep) ?

Question 3

During an investigation, you are tasked to analyze a modern Pixel phone running Android 12.0. The owner is not giving you the password/unlock code.

1. Describe different methods to get access to the data nonetheless.
    - It could be possible to trick the fingerprint sensor with a photo of the owners finger or a wax dummy of the owners finger
    - Rooting the phone is not possible without data loss since Android 7
    - Try to get the data by putting the phone in the manufacturers service mode
    - JTAG, ISP & Chip-Off (connect directly to circuit board)
    - Use TWRP (Team Win Recovery Project) = Custom recovery system (will not work without data loss)
    - Using custom bootloader (will not work without data loss)
2. Describe in your own words what a "jailbreak" is, and why it can be useful during analysis. Can you bypass a user password with a jailbreak?
    - A jailbreak means to use a exploit on iOS to unlock the root user.
3. You obtain different access tokens and passwords for online services during analysis, and are allowed to use them to retrieve data. How do you proceed?
    - Ideally use cloud forensics software to copy data
    - Try to create snapshots of the online services (if it is a Infrastructure as a Service (IaaS))
    - Also check APIs of the services which can possible contain more data
    - For PaaS (Platform as a Service) clouds deploy your own logging to analyze the system

Question 4

You are a court certified expert witness ("Sachverständige/r") and the prosecutor ("Staatsanwalt/in") asks you to join a police raid the next morning - something about an online bitcoin scam. They estimate to confiscate like 3 servers and 10 workstations, plus the smartphones of the people there.

1. How do you prepare yourself for the raid, what do you plan to take with you?
    - Bring a hardware write blocker (for readonly mode)
    - Prepare for Cold Boot Attack to dump memory of RAM
    - Bring some faraday-bags for the smartphones
2. In the basement you discover it is rather 100 servers, spread over multiple 19" racks, and more than 50 mobile phones. How do you proceed?
    - Dump RAM of everything step by step
    - Document every step
    - Unplug everything and take the hard drives
    - Try to disconnect the phones from the network as fast as possible by airplane mode and disabling WiFi, but in faraday bag if this not works

Question 5

1. Where (and how) is encryption used in modern smartphones PCs and in digital communication?
   - File-based encryption for Android phones
   - Optional on Android: Secure startup for disk encryption
   - File encryption on iOS (AES 256 crypto engine between flash storage and memory)
   - E.g. Veracrypt/Truecrypt for complete or partially encryption of PC hard drives
   - BitLocker for Windows
   - FileVault on Apple
   - dmCrypt/LUKS on Linux
   - Messenger are end-to-end encrypted (e.g. Signal) by using private/public key pairs
   - Since 2G there is also a encryption for mobile network communication (not very secure)
2. Describe use cases for both symmetric and asymmetric cryptography (in the context of digital forensics).
3. What different methods do you know to break/bypass encryption?
   - BruteForce (with masks, wordlists and patterns)
   - Avoid by doing a side attack on the hardware directly
   - Dump RAM and get encryption keys
   - Use biometric unlock by using a photo of a finger or a finger wax dummy

Question 6

You are tasked with developing a forensic app for Android and iOS. The goal is to install it on a smartphone and to automatically retrieve all files including apps and their data for creating a forensic report.

1. Which security mechanisms prevent such an app from working as intended? Describe the different security mechanisms.
   - Sandboxing: Every app has its own isolated environment, apps are unable to access others environments, apps are unable to access the systems environment
2. Which specific security mechanisms on Android and iOS prevent malicious apps/malware. Why can you not replace an already installed app with a manipulated one?
   - Android
      - APK files (i.e. App install files) signed by developer (you would need the key from the developer)
      - Signature checks verify if certificate is the same with updates
      - Asymetric/public key cryptography grants that the apk is from the given developer, grants that the apk was not tampered with
      - Can only be disabled via rooting (would means data loss)
   - iOS: Apps can only be installed via App Store
3. Describe in your own words how data encryption works on iOS (with active file protection). Is a brute force attack with a cracking server & plenty of GPUs possible?
   - iOS has a dedicated co-processor for encryption
   - Each file is encrypted by a with a file-specific key, which is encrypted with one or more of the four class keys
   - Depending on the class the files of the class are accessible or not at certain states of the device (available always, after first unlock, while device is locked but opened before, while device is unlocked)

Question 7

1. Explain the order of volatility.
   - The order of volatility is the sequence or order in which the digital evidence is collected. The order is maintained from highly volatile to less volatile data. Highly volatile data resides in the memory, cache, or CPU registers, and it will be lost as soon as the power to the computer is turned off.
2. What does pslist do? Why should you use psscan instead? Explain the differences.
   - pslist traverses the list of active process structures that the Windows kernel maintains.
   - The psscan module doesn't trust the linked list of the processes, and, instead, searches memory by heuristically looking for EPROCESS structure that represent processes.Hence, it lists all processes that are even hidden by rootkit and not shown by pslist command of volatility or tasklist command of windows. Any discrepancy between process list shown by pslist and psscan suggests that rootkit is installed.

More questions

1. What is the bitallocation map?