Windows Artifacts - Jumplists & Shortcut Files
Final Exercise Answers

1. How many shortcut files did you find within the folder “Recent”(from the archive named “SuspectActivity.zip”)?
    a. 5 shortcut files
    b. 8 shortcut files
    c. 9 shortcut files
    d.10 shortcut files (Correct Answer)

2. What was in the “Recent” folder besides the shortcut files? Select all that apply
    a. AutomaticDestinations folder (Correct Answer)
    b. A Word document
    c. CustomDestinations folder (Correct Answer)
    d. A text file

3. Which shortcut file has a modification date and time of March 26 at 11:15 PM?
    a. Antiforensics.pdf.lnk
    b. CreditCardsNumbers.txt.lnk
    c. Secret.lnk
    d. **EXFAT-251 (E).lnk** (Correct Answer)

4. What is the AutomaticDestination folder?
    a. A folder where all jump list files are located
    b. A folder where all link files are located
    c. A folder that holds user generated link files
    d. **A folder that holds system generated link** files (Correct Answer)

5. What is the CustomDestination folder?
    a. A folder where all jump list files are located
    b. A folder where all link files are located
    c. **A folder that holds user generated link files** (Correct Answer)
    d. A folder that holds system generated link files

6. What files have been accessed from the removable media connected to the computer? Select all that apply.
    a. **Antiforensics.pdf** (Correct Answer)
    b. **Bitcoins.docx** (Correct Answer)
    c. History.txt.lnk
    d. ID_Bad_Guy.png.lnk

7. What are the removable media's drive letters you found?
    a. D:
    b. F:
    c. **E:** (Correct Answer)
    d. **Z:** (Correct Answer)

8. The "Hidden.lnk" file points to a file and not a directory.
    a. True
    b. **False** (Correct Answer)

9. What is the original path for the "Hidden.lnk"?
    a. C:\Users\User\Documents\Hidden.doc
    b. **C:\Users\User\Hidden** (Correct Answer)
    c. C:\Users\User\Downloads\Hidden.pdf
    d. None of the above

10. What is the size of the target file "CreditCardsNumbers.txt"?
    a. **920 bytes** (Correct Answer)
    b. 920 KB
    c. 92 KB
    d. 92 MB

11. Which MAC addresses did you find? Select all that apply.
    a. **08:00:27:1d:b7:81** (Correct Answer)
    b. 00:e0:4c:c1:6e:f2
    c. **00:15:5d:24:f4:de** (Correct Answer)
    d. 00:00:5e:00:53:af

12. What is the Volume Label(s) of drive E:?
    a. Hidden
    b. **EXFAT-251** (Correct Answer)
    c. **ExFAT_Live** (Correct Answer)
    d. Secret

13. Were any machine IDs associated with the shortcut files? If yes, what were they?
    a. asuswin11
    b. winuser
    c. winstudent
    d. **windev2112eval** (Correct Answer)

14. Have you found any traces of VPN software being executed on the computer? If yes, what were the applications?

a. **NordVPN** (Correct Answer)
b. GoogleVPN
c. OpenVPN
d. SurfShark

15. If you found traces of a VPN software being used, which file(s) did you find it in?
    a. **2bcef060ace5a6db.customDestinations-ms** (Correct Answer)
    b. 6824f4a902c78fbd.customDestinations-ms
    c. 3c3871276e149215.customDestinations-ms
    d. 926405e5afedeeb3.customDestinations-ms (Correct Answer)

16. Have you found any traces of any remote desktop application being executed on the computer? If yes, what were they?
    a. Microsoft Remote Desktop
    b. **AnyDesk** (Correct Answer)
    c. ARD
    d. TeamViewer

17. If you found traces of a remote desktop application being used, which file(s) did you find it in?
    a. **75fdacd8330bac18.customDestinations-ms** (Correct Answer)
    b. 16f2f0042ddbe0e8.customDestinations-ms
    c. 6824f4a902c78fbd.customDestinations-ms
    d. 3c3871276e149215.customDestinations-ms

18. What was the application ID for the remote desktop application?
    a. **75fdacd8330bac18** (Correct Answer)
    b. 14354e216395983a
    c. 1bc392b8e104a00e
    d. None of the above