CIS2390 PRACTICAL ANSWERS

Week 14

Answers

1. Each MFT entry is 1024 bytes. Since 0x1400 = 5120, we have that 0x1400 is MFT entry number 5 (= 5120/1024). Entry number 5 is a NTFS metadata file called "." - ie. the root directory of the filesystem.

2. Starting at offset 0x1400 within $MFT we read out the following values for this MFT entry:

   - link count = 1, so file only has one name
   - first attribute offset = 0x38 (ie. located at offset 0x1438 within $MFT)

   Navigating through our MFT entry attributes now yields:

   - The first attribute type is $STANDARD_INFORMATION (ie. 0x10), has length 0x48 bytes (ie. next attribute starts at offset 0x1480), is resident, has no name (length is 0) and its content is at offsets 0x1450-0x147F.
   - The second attribute type is $FILE_NAME (ie. 0x30), has length 0x60 bytes (ie. next attribute starts at offset 0x14E0), is resident, has no name (length is 0) and its content is at offsets 0x-0x.
   - The third attribute type is $SECURITY_DESCRIPTOR (ie. 0x50), has length 0x48 bytes (ie. next attribute starts at offset 0x1528), is non-resident, has no name (length is 0), ...
   - The fourth attribute type is $INDEX_ROOT (ie. 0x90), has length 0x58 bytes (ie. next attribute starts at offset 0x1580), is resident, has the name $I30 (length is 4 and UNICODE name starts at 0x1540) and its content is at offsets 0x-0x.
   - The fifth attribute type is $INDEX_ALLOCATION (ie. 0xA0), has length 0x50 bytes (ie. next attribute starts at offset 0x15D0), is non-resident, has the name $I30 (length is 4 and UNICODE name starts at 0x15C0), ...
   - The sixth attribute type is $BITMAP (ie. 0xB0), has length 0x28 bytes (ie. next attribute starts at offset 0x15F8), is resident, has the name $I30 (length is 4 and UNICODE name starts at offset 0x15E8) and its content is at offsets 0x-0x.
   - The seventh attribute starts with 0xFFFFFFFF and so marks the end of this MFT entry's attribute list.

3. A search of the $MFT file for the UNICODE string *file-r-1.dat* reveals that only the MFT entry at offset 0x6C00 contains this string. This entry has the following attributes:

   - 0x6C38: $STANDARD_INFORMATION[resident]
   - 0x6C98: $FILE_NAME[resident]

- 0x6D10: $DATA[resident] (no name - ie. default data stream)
- 0x6DA0: 0xFFFFFFFF - ie. end of attribute list

From resident attribute header, we have that 0x6D10 content is at 0x6D28-0x6D9F.

4. A search of the $MFT file for the UNICODE string *file-n-5.dat* reveals that only the MFT entry at offset 0x9400 contain this string. This entry has the following attributes:
   - 0x9438: $STANDARD_INFORMATION[resident]
   - 0x9498: $FILE_NAME[resident]
   - 0x9510: $DATA[non-resident] (no name - ie. default data stream)
   - 0x9558: $DATA[non-resident] (named “here” [UNICODE name is length 4 and starts at 0x9598] - ie. an alternate data stream) content is 0x7D0 bytes in size
   - 0x95B0: 0xFFFFFFFF - ie. end of attribute list

   From non-resident attribute header, we have that 0x9558 content is determined by information stored within the runlist that starts at 0x95A0. This runlist has the following data:
   - 0x95A0: offset size = 2B (= 0x14E8); length size = 1B (= 2 clusters); so runlist is 4B in size (ie. next runlist is at 0x95A4); thus clusters 0x14E8 to (0x14E8+0x2) make up this runlist
   - 0x95A4: offset size = 2B (= 0x0A9A); length size = 1B (= 2 clusters); so runlist is 4B in size (ie. next runlist is at 0x95A8); thus clusters (0x14E8+0x0A9A) to (0x14E8+0x0A9A+0x2) make up this runlist
   - 0x95A8: this is a null byte and indicates the end of the runlist records.

   So, we have that the “*file-n-5.dat:here*” ADS content is stored in the first 2000 bytes of clusters 5352-5353 and 8066-8067.