UNIVERSITY OF WOLVERHAMPTON

6CS010 Digital Forensics

Revision

Module content

- Principles of digital investigation
- Understanding digital data
- Data storage
  - Disks
  - File systems
  - Volatile data
  - Internet data
  - Mobile data
- Forensic challenges

UNIVERSITY OF WOLVERHAMPTON

Coursework

1. To develop an Expert Report template using MS word. Z-Security wants a new template to standardise and use for this investigation to maintain cross-team consistency in their documentation. The template should include suitable branding, titles, subtitles and notes. *[should not exceed 3 pages]*
2. To conduct a literature review and critically discuss published Digital Investigation Process Models. The narrative should compare and conclude (with justification) the most suitable model for Z-Security to adopt. Examples of criterions to support your conclusion include but not limited to the module's ability to cover new technologies (e.g. IoT), flexibility, and to support the team's collaborative activities. This discussion must be referenced throughout. *[Word count (excluding references): 500 words ± 10%]*
3. To perform full analysis on a byte-to-byte copy of the given asset; machine's hard drive and memory (volatile data). The asset can be found on Canvas as a VM (VM-SnapshotSep2016.7z) As a Digital Investigator, you are expected to work within the guidance of a forensic model to report your findings. You must discover, document and forensically report any four actions performed on the seized device in violation of UBB's Acceptable Use Policy (AUP) which can be found in Appendix 1. Your work during the investigation should consider the rigour, reproducibility and integrity of data. Any findings that could help attributing these actions to an individual or more will be relevant as well. *[no wordcount or maximum number of pages, but do not document more than two unacceptable actions]*
4. To develop a Digital Investigation Toolkit prioritising open-source tools. These tools will be utilised by you for this incident to perform the required analysis (i.e. for the specific type of technology you will investigate, everything else is out of scope), or to be used by any Z-Security team in the future for the same type of investigation. The Toolkit should be presented within a table and supported by any brief notes deemed necessary. *[2-3 pages]*

Exam preparation

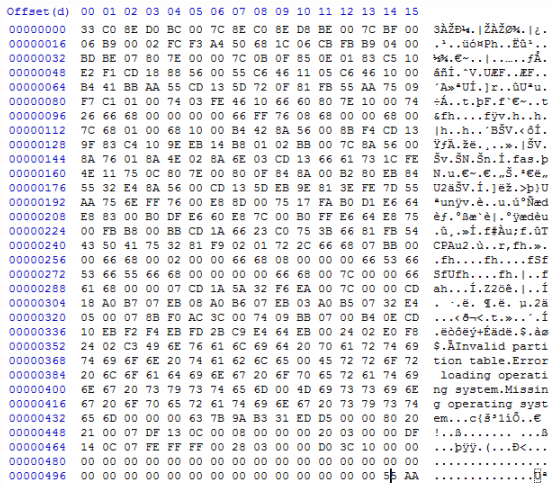
- Re-visit again all the content posted for Weeks 1 to 12.
- Study the slides in this presentation as it includes additional material to support your preparation
  - When a topic is mentioned, locate its material from weeks 1 to 11
- Attempt the Mock Exam
  - You should answer all questions so that we can discuss your answers together and think of how you can improve them.

Examples of Important Topics

- Forensics Guidelines
  - ACPO principles
  - Why do we need to consider the ACPO principles in forensics investigations? Examples..
- MBR
  - What is the Master Boot Record (MBR) in a computer system?
  - Is there an alternative option to use?

Example of Important topics

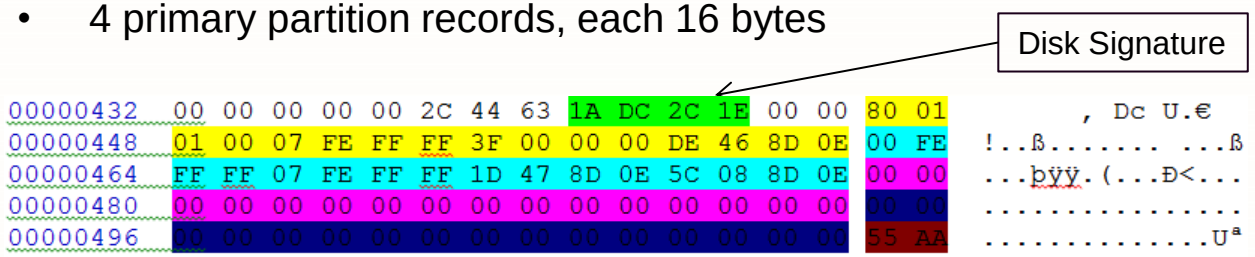
- Physical sector/LBA 0
- Size= 512 bytes
- Contents include
  - Boot code
  - Disk signature
    - 4 bytes from offset 440
  - Master Partition Table (MPT)
    - From offset 446
    - Allows 4 Primary partitions
  - Signature of ‘55AA’
    - Offset 510 &511



Offset(d)	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
00000000	33	C0	8E	D0	BC	00	7C	8E	C0	8E	D8	BE	00	7C	BF	00
00000016	06	B9	00	02	FC	F3	A4	50	68	1C	06	CB	FB	B9	04	00
00000032	BD	BE	07	80	7E	00	00	7C	0B	0F	85	0E	01	83	C5	10
00000048	E2	F1	CD	18	88	56	00	55	C6	46	11	05	C6	46	10	00
00000064	B4	41	BB	AA	55	CD	13	5D	72	0F	81	FB	55	AA	75	09
00000080	F7	C1	01	00	74	03	FE	46	10	66	60	80	7E	10	00	74
00000096	26	66	68	00	00	00	00	66	FF	76	08	68	00	00	68	00
00000112	7C	68	01	00	68	10	00	B4	42	8A	56	00	8B	F4	CD	13
00000128	9F	83	C4	10	9E	EB	14	B8	01	02	BB	00	7C	8A	56	00
00000144	8A	76	01	8A	4E	02	8A	6E	03	CD	13	66	61	73	1C	FE
00000160	4E	11	75	0C	80	7E	00	80	0F	84	8A	00	B2	80	EB	84
00000176	55	32	E4	8A	56	00	CD	13	5D	EB	9E	81	3E	FE	7D	55
00000192	AA	75	6E	FF	76	00	E8	8D	00	75	17	FA	B0	D1	E6	64
00000208	E8	83	00	B0	DF	E6	60	E8	7C	00	B0	FF	E6	64	E8	75
00000224	00	FB	B8	00	BB	CD	1A	66	23	C0	75	3B	66	81	FB	54
00000240	43	50	41	75	32	81	F9	02	01	72	2C	66	68	07	BB	00
00000256	00	66	68	00	02	00	00	66	68	08	00	00	00	66	53	66
00000272	53	66	55	66	68	00	00	00	00	66	68	00	7C	00	00	66
00000288	61	68	00	00	07	CD	1A	5A	32	F6	EA	00	7C	00	00	CD
00000304	18	A0	B7	07	EB	08	A0	B6	07	EB	03	A0	B5	07	32	E4
00000320	05	00	07	8B	F0	AC	3C	00	74	09	BB	07	00	B4	0E	CD
00000336	10	EB	F2	F4	EB	FD	2B	C9	E4	64	EB	00	24	02	E0	F8
00000352	24	02	C3	49	6E	76	61	6C	69	64	20	70	61	72	74	69
00000368	74	69	6F	6E	20	74	61	62	6C	65	00	45	72	72	6F	72
00000384	20	6C	6F	61	64	69	6E	67	20	6F	70	65	72	61	74	69
00000400	6E	67	20	73	79	73	74	65	6D	00	4D	69	73	73	69	6E
00000416	67	20	6F	70	65	72	61	74	69	6E	67	20	73	79	73	74
00000432	65	6D	00	00	00	63	7B	9A	B3	31	ED	D5	00	00	80	20
00000448	21	00	07	DF	13	0C	00	08	00	00	00	20	03	00	00	DF
00000464	14	0C	07	FE	FF	FF	00	28	03	00	00	D0	3C	10	00	00
00000480	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000496	00	00	00	00	00	00	00	00	00	00	00	00	00	00	55	AA

Examples of Important Topics

- Starts at byte/offset 446 in the MBR
- 4 primary partition records, each 16 bytes



- Byte 1:'**80**' is bootable otherwise '**00**'
- Bytes 2-4: start sector (CHS)
- Byte 5: partition type
- Bytes 6-8: last sector (CHS)
- Bytes 9-12: start sector (LBA)
- Bytes 13-16: size in sectors

The generic 64-byte Primary Partition Table

Offsets within MBR sector		Length (in bytes)	Contents
Dec	Hex		
446 – 461	1BE - 1CD	16	Table Entry for Primary Partition # 1
462 – 477	1CE - 1DD	16	Table Entry for Primary Partition # 2
478 – 493	1DE - 1ED	16	Table Entry for Primary Partition # 3
494 - 509	1EE - 1FD	16	Table Entry for Primary Partition # 4

Calculate the size of the partition in bytes

- A sample partition table entry is shown below:
  - 80 20 21 00 07 7E 25 19 00 08 00 00 **00 32 06 00**
  - The underlined hex values (in little endian format) gives the number of 512Kb sectors in the partition. Calculate the size of the partition in bytes.
- Solution
  1. Since the value is stored in Little endian format the number should be read from right-to-left, therefore 00 32 06 00 becomes 00 06 32 00 hex
  2. Then, convert to from hex values to decimal; 00 06 32 00 hex = 406,016 decimal. This gives you the number of sectors.
  3. Finally, since the size of each sector is 512 bytes, you can calculate the size in byes; 406,016 x 512 = **207,880,192 bytes**

Examples of Important Topics

- Forensics Investigation Models
  - Stages and steps to analyse and locate data of interest
  - Acquisition process
- Filesystems
  - FAT
  - NTFS
    - MFT
    - MFT file record

UNIVERSITY OF WOLVERHAMPTON

NTFS File Record

```
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

46 49 4C 45 30 00 03 00 5C 2F 40 00 00 00 00 00   FILE0...\/@.....
01 00 01 00 38 00 01 00 60 01 00 00 00 04 00 00   ....8...`.......
00 00 00 00 00 00 00 00 05 00 00 00 26 00 00 00   ............&...
07 00 00 00 00 00 00 00 10 00 00 00 60 00 00 00   ............`...
00 00 00 00 00 00 00 00 48 00 00 00 18 00 00 00   ........H.......
70 D7 96 E5 E1 AD D6 01 74 C8 11 EE E1 AD D6 01   p×-åá.Ö.tÈ.îá.Ö.
74 C8 11 EE E1 AD D6 01 74 C8 11 EE E1 AD D6 01   tÈ.îá.Ö.tÈ.îá.Ö.
20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ...............
00 00 00 00 08 01 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 30 00 00 00 70 00 00 00   ........0...p...
00 00 00 00 00 00 03 00 54 00 00 00 18 00 01 00   ........T.......
05 00 00 00 00 00 05 00 70 D7 96 E5 E1 AD D6 01   ........p×-åá.Ö.
70 D7 96 E5 E1 AD D6 01 70 D7 96 E5 E1 AD D6 01   p×-åá.Ö.p×-åá.Ö.
70 D7 96 E5 E1 AD D6 01 00 00 00 00 00 00 00 00   p×-åá.Ö.........
00 00 00 00 00 00 00 00 20 00 00 00 00 00 00 00   ........ .......
09 00 46 00 69 00 6C 00 65 00 31 00 2E 00 74 00   ..F.i.l.e.1...t.
78 00 74 00 00 00 00 00 40 00 00 00 28 00 00 00   x.t.....@...(...
00 00 00 00 00 00 04 00 10 00 00 00 18 00 00 00   ................
02 DF 4D CE C9 19 EB 11 9C EE 5C 26 0A 1A 26 D6   .ßMÎÉ.ë.œî\&..&Ö
80 00 00 00 28 00 00 00 00 00 18 00 00 00 01 00   €...(...........
0B 00 00 00 18 00 00 00 48 65 6C 6C 6F 20 57 6F   ........Hello Wo
72 6C 64 00 00 00 00 00 FF FF FF FF 82 79 47 11   rld.....ÿÿÿÿ‚yG.
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
```

Header 0100 current file, 00 deleted

(10 00 00 00) $Standard Information

(30 00 00 00) $File_Name

(40 00 00 00) $Object_ID

(80 00 00 00) $Data

Examples of Important Topics

- Forensics challenges
- Antiforensics
  - Categories/ techniques
  - Examples
  - Critic

Good Luck ☺