Introduction to Computer Forensics and Security

"How to Revise"

School of Computing, Mathematics & Digital Technology

Manchester Metropolitan University.

How to Revise

- Unit Learning Resources (lecture notes and lab handouts)
- Highlighted Topics Areas
- Past Exams!!

Unit Learning Resources

Week 1 - Induction and Introduction to Computer Forensics

This week lectures will introduce the following:

The unit structure, specification and assessment; what is digital forensics; basics of crimes, historical perspectives to cyber security and types of criminal cases and the usefulness of having digital forensics as a field of work.

The lab exercises will introduce a leading digital forensics platform which is EnCase. Manchester Met. is an academic partner with Guidance Software which produced EnCase. The lab exercises will be based on Guidance Software Industry training programme as part of the partnership agreement.

- ♣ I Lecture 1 Introduction to Computer Forensics
- 💠 🔳 Lab EnCase Industry Training Creating Case 🞤
- ♣ I Lab EnCase Industry Training Navigating EnCase V7
- ♣ Introduction to EnCase V6 & V7
 ♣
- ♣ Lab-Forensic-Image-Intermediate-USB32.E01
- + Extra EnCase V6 Manual
- 🛊 🧾 Extra EnCase V7 Manual 🎤
- ♣ EnCase V8 New Features Guideline ▶
- Reading list:

Pages (3-31) Computer Forensics Principles and Practices Pages (39 - 46, 49 - 50) Computer Forensics Principles and Practices

Highlighted Topics Map

Final Exam List Revision:

White: Background Reading. Yellow: Define, explain etc.

Red: Detailed understanding, reasoning and critical analysis.

Forensic Computing Basics of Crimes *

What constitutes a crime and identify categories of crime *

Cybercrime Categories * Civil vs. Criminal Charges

Computer Forensics Skills

Types of Evidence *

Law enforcement's authority

Computer Forensics Can Reveal

Discovery Process

Different types of evidence *

What affects the admissibility of evidence.

Knowing What to Look For

Admissibility of Evidence *

Forensics Investigation Methods

How electronic evidence differs from physical evidence

What computer forensics tools and techniques can reveal and recover,

The process of discovery and electronic discovery

Volatile Information & Nonvolatile Information * Volatile Information ***

ACPO guidelines ***
Forensic computing process ***

Past Exams

Assessments

Help files, Assignments and Past Exams.



Final Exam for the Academic Year 2014-2015



Final Exam for the Academic Year 2015 - 2016

- 🛂 Important Exam Highlighted Revision List 2017 2018 🎤
- 🛂 Final Exam for the Academic Year 2014-2015 🎤
- Final Exam Solutions for the Academic Year 2014-2015 >
- 🔼 Final Exam for the Academic Year 2015 2016 🎤
- 🛂 Final Exam Solutions for the Academic Year 2015 2016 🎤
- Introduction to Computer Forensics and Security Exam 2016-2017 >
- Introduction to Computer Forensics and Security Exam Solutions 2016-2017



🗖 Library

Full Reading List

Essential (17)

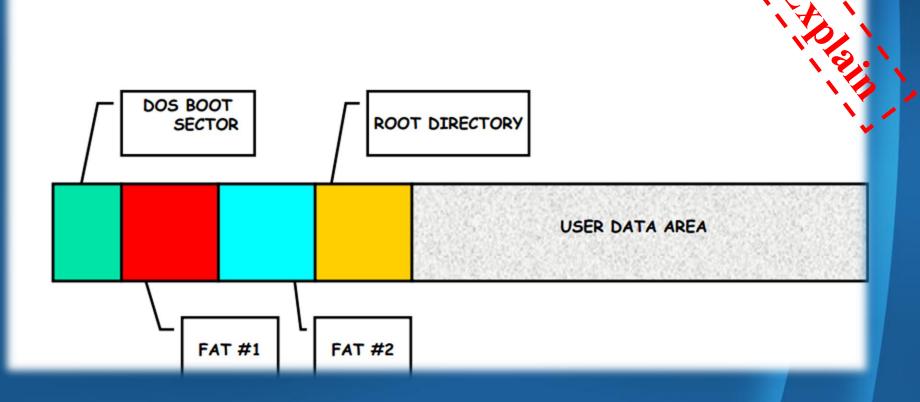
Files (0)

Exam papers (2)

2012 summer

2011 summer

FAT12/16 Structure



Master Boot Record



```
OOOEB 3C 90 4D 53 44 4F 53 35 2E 30 00 02 01 01 00 02 E0 00 40 0B F0
02209 00 12 00 42 00 00 00 00 00 00 00 00 00 00 29 DD 16 15 24 4E
0444F 20 4E 41 4D 45 20 20 20 20 46 41 54 31 32 20 20 20 FA 33 CO 8E
066D0 BC 00 7C 16 07 BN 78 00 36 C5 37 1K 56 16 53 BF 3K 7C B9 0B 00
088FC F3 A4 06 1F C6 45 FF OF 8B OE 18 7C 88 4D F9 89 47 02 C7 07 3E
1107C FB CD 13 72 79 33 GQ 39 6 13 7C 74 08 8B 0E 13 7C 89 0E 20 7C | (M·ry3@9··|t····|
132A0 10 7C F7 26 16 2 06 1C C 13 16 1E 7C 03 06 0E 7C 83 D2 00
154A3 50 7C 89 16 52 7C 43 9 7C 89 18 4B 7C B8 20 00 F7 26 11 7C 8B #P| R|#I| R|8 W4 |
1761E 0B 7C 03 C3 48 F7 F3 1 0 4 7C 8 16 4B 7C 00 BB 00 05 8B 16
19852 7C A1 50 7C E8 92 00 72 1
                                  1 E8 AC 00 72 16 8B FB B9 0B 00
220BE E6 7D F3 A6 75 0A 8D 7F Q B9 07 7 3 A6 4 18 BE 9E 7D E8 5F >f)squ 0 9 · · sqt · > · )h
24200 33 C0 CD 16 5E 1F 8F 04 8F 44 02 10 19 56 58 88 EB E8 8B 47 1A
26448 48 8A 1E OD 7C 32 FF F7 E3 03 0 49 7 3 16 4B 7 BB 00 07 B9 HH · |2|wc·I|··K|;··9
28603 00 50 52 51 E8 3A 00 72 D8 B0 01 E8 54 00 59 51 58 72 BB 05 01
                                                                    · · PRQh: ·rX0·hT·YZXr; · ·
30800 83 D2 00 03 1E 0B 7C E2 E2 8A 2E 15 7C 8A 14 4 7C 8B 1E 49 7C
330A1 4B 7C EA 00 00 70 00 AC 0A CO 74 29 B4 0E B 07 00 0 10 EB F2 !K|j.p., @t)4.;..M.kr
3523B 16 18 7C 73 19 F7 36 18 7C FE C2 88 16 4F 7C 🛰 DZ 🙌 🧽 1A 7C
37488 16 25 7C A3 4D 7C F8 C3 F9 C3 B4 O2 8B 16 4D 7C 🖎 06 🞾 📂 0A
39636 4F 7C 8B CA 86 E9 8A 16 24 7C 8A 36 25 7C CD 13 C3 ON OA
4186K 2D 53 79 73 74 65 6D 20 64 69 73 6B 20 6F 72 20 64 69 73 6B 20
44065 72 72 6F 72 0D 0A 52 65 70 6C 61 63 65 20 61 6E 64 20 70 72 55 error Replace and pre
46273 73 20 61 6E 79 20 6B 65 79 20 77 68 65 6E 20 72 65 61 64 79 0D 🗫 any key when ready
4840A 00 49 4F 20 20 20 20 20 20 53 59 53 4D 53 44 4F 53 20 20 20 53
                                                                              SYSMSDOS
50659 53 00 00 55 👪
                                                                    YS··U™
```

```
00041 74 00 65 00 73 80 74 00 66 00 0F 00 8C 6F 00 6C 00 64 00 65 00 72 00 Atterstf...Dorl.d.e.r.
02400 00 00 00 EF FF FF FF 54 45 53 54 46 4F 7E 31 20 20 20 10 00 3C 23 96 ····ÿÿÿŢESTFO~1
04839 3B 39 3B 0 00 24 6 39 3B 02 00 00 00 00 00 41 74 00 65 00 73 00 74 9;9;····$|9;·····At·e·s·t
07200 66 00 07,00 2C 6F 00 67 90 64 06 65 00 72 00 31 00 00 00 00 FF FF .f...,o.1.d.e.r.
09654 45 53 54 46 4F 7E 52 10 27 20 10 00 40 2B 96 39 3B 39 3B 00 00 2C 96 TESTF0~2 ...@+|
50400 00 00 00 00 00 00 00
```

- Critically highlight the forensic value of the following:
 - Thumbs.db
 - etc

Questions?

m.owda@mmu.ac.uk