Digital Evidence and Computer Crime

Course Work: Component-B

Deliverables

Details	Marks
Contemporaneous Notes	30
Report Writing	40
Timeline	15
Opinion	15
Total	100

Coursework info (1)

Ensure you have run ALL related *Evidence Processor* modules before submitting:

- Recover Folders (find deleted files)
- File signature analysis (find file mismatch instances)
- Protected file analysis
- Thumbnail creation (look at thumbs.db artefacts)
- Hash analysis (use the entropy function to find files with large entropy)
- Expand compound files (expand files such as zip, etc.)
- Find email (look for exchanged emails)
- Find Internet artifacts (look for artefacts derived from internet activity)
- Search for keywords (or just create an index)
- Index text and metadata
- Personal Information (might create a lot of false positives)
- System Info Parser (information related to the Registry)
- IM Parser (find messenger instant messenger artefacts)
- File Carver (if you wish to parse the unallocated space)
- Windows Event Log Parser (information derived from the Windows event logs)
- Windows Artifact Parser (find .lnk files and other Windows artefacts)

Coursework info (II)

Contemporaneous Notes

Action	Done?	Date	Time	Notes
Load case & verify image				
Recover lost folders (FAT16 & 32). Mount archives; zip, thumbs.db, etc. File signature analysis, compute hash values				
Perform data carving				
Retrieve operating system information, accounts information, software, time zone information etc.).				
Timeline analysis - Note date of last activity on the computer.				

Which module did you use? Did you make any additional settings?

Did you perform Data Carving? Which file types did you try to recover?

Don't forget to use the description given from EnCase for each module

Also useful for your Timeline section

Coursework info (III)

Contemporaneous Notes

Action	Done?	Date	Time	No
Log-on passwords – use SAMInside/Ophcrack/Encase				
Registry analysis and Registry protected area				
Internet History, favourites. Other browsers?				
Run relevant keyword searches				
Emails, local & web-based.				
IM clients				

Which module did you use? Did you perform any additional actions?

Which keywords did you use? Why? Did you index your data?

Which module did you use? Did you find any interesting results?

Coursework info (IV)

REPEATABILITY

Contemporaneous Notes

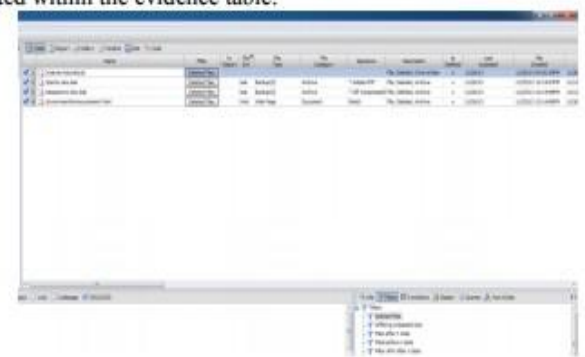
Internet History, favourites. Other browsers?				
Run relevant keyword searches				
Emails, local & web-based.				
IM clients				
Examine different file types. Export doc / office & exe files; look at Meta data if required				
Clean-up utilities. Check log files				
Encryption, Steg				

Which module did you use? Any interesting interactions?

Have you done file signature analysis?

Have you seen anything of interest? No need to invest time on Crypto.

Contemporaneous Notes (V)

Action	Done?	Date	Time	Notes	Initial
Load case & verify in EnCase	YES	11.03.14	10.35am	- Loaded E01 File into Encase - Created a case by entering case details - Encase automatically verified case Verification MD5 38e569d0fe655ade6a3a84fd3987f8bb 	LG
Recover lost folders (FAT16 & 32).	YES	11.03.14	10.36m	- Within Encase used the filter function to retrieve any files that were deleted (shown in image below). - The results showed four deleted files, three of which were evidence items and are stated within the evidence table.  	LG

Coursework info (VI)

Report – See also *Casey (2011)*, Section 16.7.

- Around 4-5 pages long and will document the most significant evidence items.
- Include a provenance block for each item, probably in an Appendix (you can use the Autopsy automated reporting function).

DOCUMENT FACTS

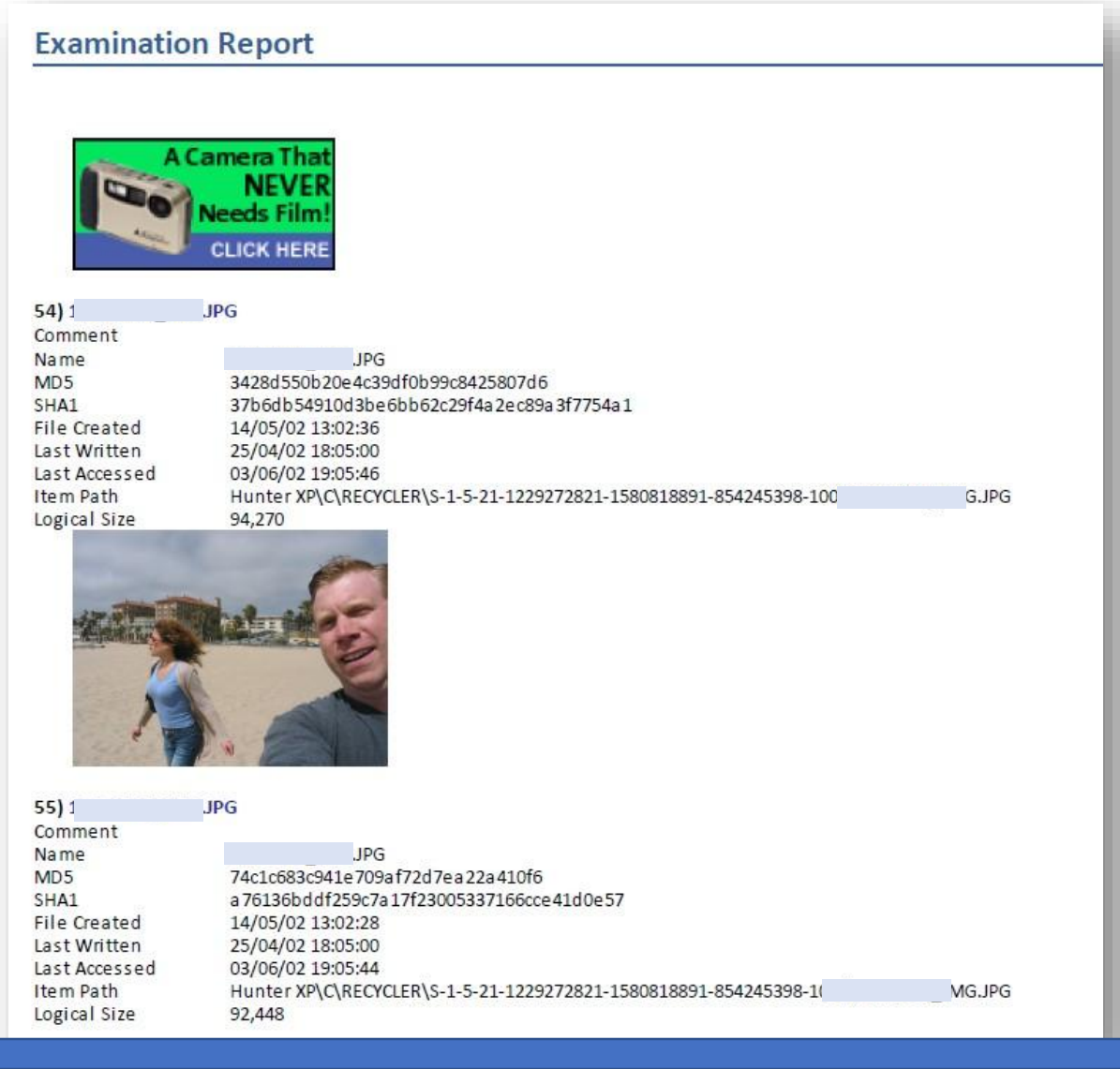
FULL PROVENANCE

Coursework info (VII)

Report –

Appendix –

Provenance



Examination Report

54) 1 JPG

Comment	
Name	JPG
MD5	3428d550b20e4c39df0b99c8425807d6
SHA1	37b6db54910d3be6bb62c29f4a2ec89a3f7754a1
File Created	14/05/02 13:02:36
Last Written	25/04/02 18:05:00
Last Accessed	03/06/02 19:05:46
Item Path	Hunter XP\C\RECYCLER\S-1-5-21-1229272821-1580818891-854245398-100 G.JPG
Logical Size	94,270

55) 1 JPG

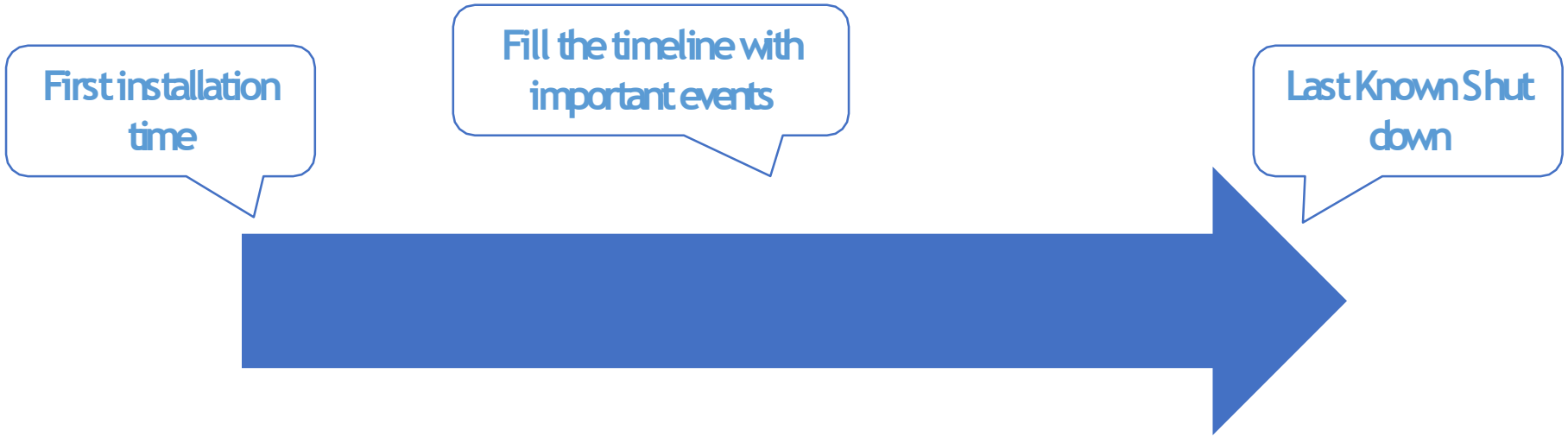
Comment	
Name	JPG
MD5	74c1c683c941e709af72d7ea22a410f6
SHA1	a76136bddf259c7a17f23005337166cce41d0e57
File Created	14/05/02 13:02:28
Last Written	25/04/02 18:05:00
Last Accessed	03/06/02 19:05:44
Item Path	Hunter XP\C\RECYCLER\S-1-5-21-1229272821-1580818891-854245398-1(MG.JPG
Logical Size	92,448

Coursework info (VIII)

Timeline

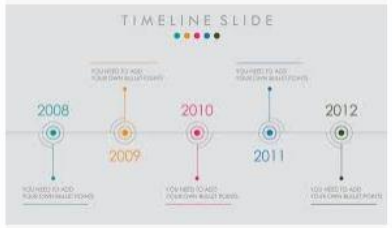
- You can be creative!
- You can provide a nice visualisation.

- An example:

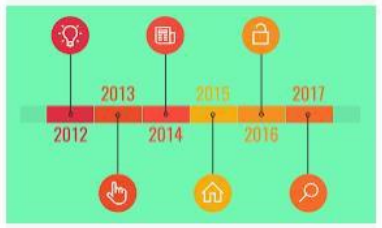


Timeline – a simple web search

Marvel Cinematic Universe Timeline
officetimeline.com

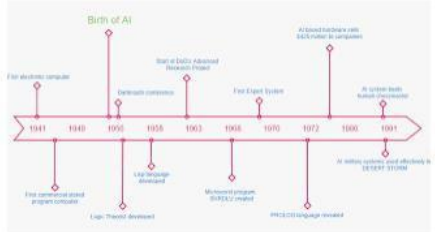


Animated PowerPoint Timeline Template ...
powerpointschool.com

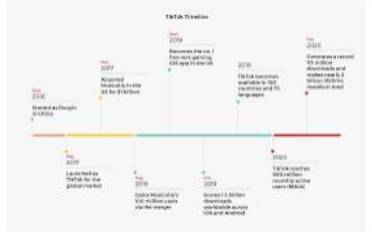


Timeline Template Examples and Design ...
venngage.com

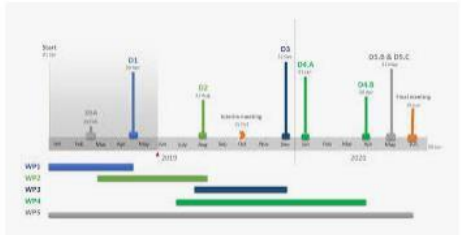
History timeline
templates.office.com



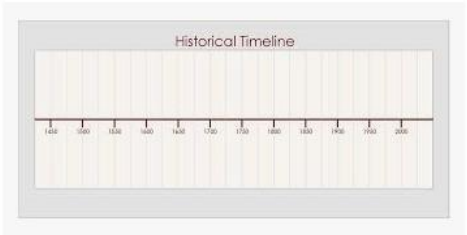
What is Timeline Diagram? (With Examples)
online.visual-paradigm.com



A visual timeline of TikTok's rise ...
techinasia.com



Timeline | CROS
ec.europa.eu

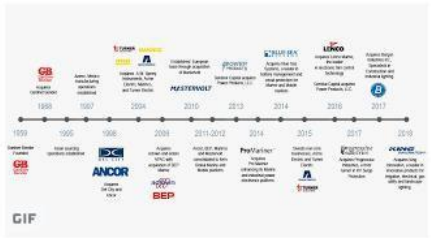


Timeline - Island of the Blue Dolphins ...
nps.gov

Proposal Timeline ...
rfp360.com

Timeline Images, Stock Photos & Vectors ...
shutterstock.com

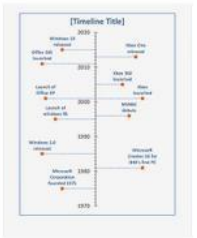
Office Timeline Add-in - Plus Edition
officetimeline.com



Timeline
ecmindustries.com

Timeline Images | Free Vectors, Stock ...
freepik.com

IMT recruitment timeline
imtrecruitment.org.uk



Vertical Timeline
templates.office.com

coronavirus pandemic – a timeline ...
weforum.org

Timeline Template Examples ...
venngage.com

7 Timeline Infographic Templates to ...
visme.co

Source: https://www.google.com/

Coursework info (IX)

Opinion

- Accumulate the results of your research in this section to state your opinion about what happened and state if there exist crimes committed by individuals.
- You can refer to relevant legislation, e.g. U.K. law

STATE YOUR OPINION ABOUT THE CASE

Coursework (1)

- Check assessment specification on blackboard!!! (Assignments folder)
- You should:

Deliverables

a) Investigate the evidence (Hunter XP case) for potential criminal activity.

b) Keep contemporaneous **notes** of your examination. (30%)

c) Write a report presenting **the facts** you have discovered; (40%)

d) Create a **timeline** of the sequence of **significant events** in the case. (15%)

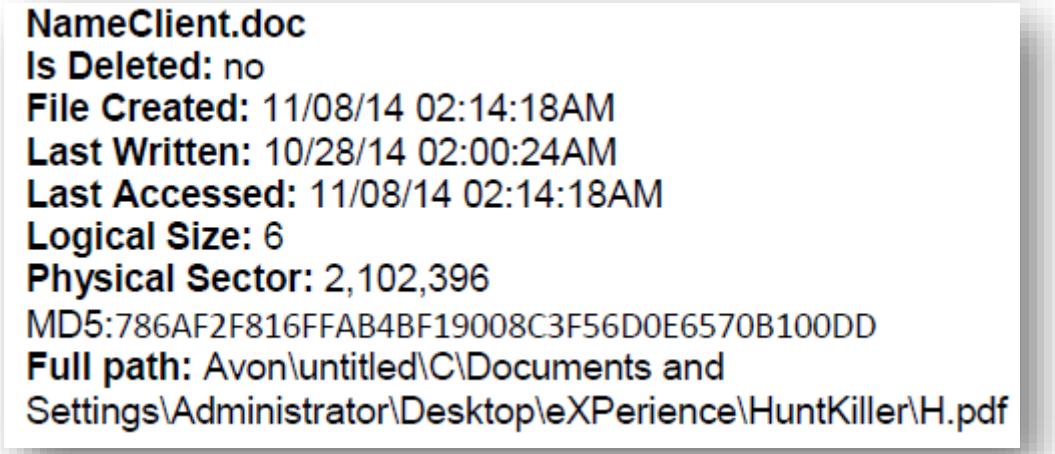
e) Write a brief summary of **your opinion** of what occurred, based on the facts you discovered (15%).

Coursework (II)

- Keep contemporaneous **notes** of your examination. (30%)
  - ✓ Record INPUT and OUTPUT → ACTION and RESULT
  - ✓ Ensure REPEATABILITY!
- Write a report presenting **the facts** you have discovered; (40%)
  - ✓ Provide pointers to the Provenance Block (listed in an Appendix)
  - ✓ Be IMPARTIAL!
- Create a **timeline** of the sequence of **significant events** in the case. (15%)
  - ✓ Document important events!
- Write a brief summary of **your opinion** of what occurred, based on the facts you discovered (15%).

Coursework (III)

- Use the EnCase Examination Report to provide the provenance blocks (or another tool, e.g. Autopsy)
- Include useful details, such as:



- **Upload your submission as a ZIP FILE on Blackboard. BEFORE the deadline 14th January 2021 - 14:00!**

The coursework deadline is approaching…