In this 4-week module, the aim is to introduce you to some key concepts and techniques which you can use to develop your own knowledge and procedures for forensic analysis. Because we're dealing with cyber security incidents, we'll concentrate on repsonding to incidents and the use of "dead box" forensic techniques (i.e. those where we can seize a device and take an image of its secondary storage devices in particular).

There will be a lot of hands-on exercises which will run on cloud-based Virtual machines, but if you want the software for yourself, we'll be using the [**CAINE 11 forensic toolkit**](https://www.caine-live.net/) with the addition of the older [Win-UFO toolkit.](https://web.archive.org/web/20150330135427/http%3A/win-ufo.org/downloads.shtml) (Note - the Windows tools require admin. privileges and WILL trigger malware warnings or be blocked by most Windows malware protection systems. The Linux live distribution is equally dangerous...)

It would also be beneficial if you could spend a bit of time revising the following key concepts:

* CPU architecture, including data representation (bit patterns and their interpretations) and Direct Memory Access. (Tarnoff Chapters 2,3 and 15)
* Operating system functions - resource management, scheduling, memory management (Dusseau & Dusseau Chapters on Virtualization)
* Discs and file systems - sectors, partitions, clusters/minimum allocation units. (Dusseau and Dusseau chapters 35 to 40).

The free online books below may help:

**Computer Architecture and O/S revision**

[Tarnoff: Computer Organization and Design Fundamentals](http://faculty.etsu.edu/tarnoff/ntes2150.html)

[Dusseau and Dusseau : Operating Systems, 3 easy pieces](http://pages.cs.wisc.edu/~remzi/OSTEP/)

**Learning materials and schedule**

As always, the learning materials, lab and exercises will be released in advance, and the plan is to have video walk-throughs of each lab. Exercise: you can use if you get stuck (and to prove that the exercises have been tested) The Week numbers are suggestions - feel free to work faster if you want to, but you should aim to complete each block of material by the end of the week that contains it.

**Task**

The task will be in two parts

* Part 1: the investigation of an incident and the potential digital evidence associated with it. (You will be provided with an image file to analyse). You will be required to produce a forensic analyst's report for this.
* Part 2: preparation of a detailed plan, containing recommended actions to take to carry out a proper investigation of related or similar incidents occurring in the organisation described in the scenario for part 1.

It will be possible to complete Part 1 using only the tools provided to you in the virtual machines. Part 2 will require some further reading.

**This folder**

The folder containing this message will be where any extra reference material or links to interesting/useful things (not used elsewhere in the module) will appear.

# ISO/IEC standards

ISO/IEC 27037, 27041, 27042 and 27043 are particular useful for this module - and the model they present is used as the basis for the recommended structure of a digital investigation. You can obtain copies via the University Library's subscription to [BSI online](http://libproxy.york.ac.uk/login?url=https://bsol.bsigroup.com/MyBsol/MyCustomCollection?subscriptionUid=45059463-a9ab-4a6b-a2cf-d35e706c3367)

27040, on storage security, also has some relevance to preservation, redaction and destruction considerations.

# Selected Reference material

This is a slightly random selection, and their inclusion here is not necessarily an indication of their relative importance, or of the scope of the module. They may be harder to locate than some of the references, or a better reference for the topic than you might find via a simple Google search.

* **The PDF files are in the directory**
* ACPO Good Practice Guide Version 5
* ASCII Code Table
* ATA-6 Attachment Specification
* File Signatures (see below)
* Forensically Interesting Spots in the Windows 7 File System and Registry
* Guidance for Experts
* How Unique Is Your Web Browser
* Into the boxes Jan 2010 (User assist Keys)
* Private browsing A window of forensic opportunity
* The joys of complexity and the deleted file
* The Meaning of LIFE (Linkfiles)
* Time and date issues in forensic computing - a case study
* US Department of Justice - Forensic Examination of Digital Evidence
* **Use links below to access these two below:**
* [Don't trust spell cheques](https://web.cs.dal.ca/~johnston/poetry/spellchecker.html)
* [The Forensics Wiki](https://forensicswiki.xyz/page/Main_Page)

# File Signatures Table

(Thanks to Gary Kessler for making this available to the community - the most up to date copy of this information can be found at his website: <https://www.garykessler.net/library/file_sigs.html> ).

This table of file signatures (aka "magic numbers") is a continuing work-in-progress. I have found little information on this in a single place, with the exception of the table in Forensic Computing: A Practitioner's Guide by T. Sammes & B. Jenkinson (Springer, 2000); that was my inspiration to start this list in 2002. See also Wikipedia's [List of file signatures](http://en.wikipedia.org/wiki/List_of_file_signatures). Comments, additions, and queries can be sent to Gary Kessler at gck@garykessler.net.

This list is not exhaustive. Interpret the table as the magic number generally indicating the file type rather than the file type always having the given magic number. If you want to know to what a particular file extension refers, check out some of these sites:

* [File Extension Seeker: Metasearch engine for file extensions](http://file-extension.net/seeker/)
* [FILExt.com](http://filext.com/)
* [FileInfo.com](http://www.fileinfo.com/)
* [Wotsit.org](http://www.wotsit.org/), The Programmer's File and Data Resource
* [DOT.WHAT?](http://www.dotwhat.net/)
* [File-Extensions.org](http://www.file-extensions.org/)

Some other useful information:

* The [File Signatures Web site](http://www.filesignatures.net/) searches a database based upon file extension or file signature.
* Check out Tim Coakley's [Filesig.co.uk](http://www.filesig.co.uk/) site, with Filesig Manager and Simple Carver. Also, see Tim's [SQLite Database Catalog page](http://www.filesig.co.uk/sqlitedatabasecatalog/), "a repository of information used to identify specific SQLite databases and properties for research purposes."
* See Marco Pontello's [TrID - File Identifier](http://mark0.net/soft-trid-e.html%22%20%5Ct%20%22_blank), a utility designed to identify file types from their binary signatures.
* My [software utility page](http://www.garykessler.net/software/index.html#filesigs) contains a custom signature file based upon this list, for use with FTK, Scalpel, Simple Carver, Simple Carver Lite, and TrID.
* Additional details on graphics file formats can be found at [The Graphics File Formats Page](http://www.dcs.ed.ac.uk/home/mxr/gfx/2d-hi.html) and the [Sustainability of Digital Formats Planning for Library of Congress Collections site](http://www.digitalpreservation.gov/formats/fdd/still_fdd.shtml).
* Additional details on audio and video file formats can also be found at the[Sustainability of Digital Formats Planning for Library of Congress Collections site](http://www.digitalpreservation.gov/formats/fdd/browse_list.shtml).
* Another collection of many types of file format specifications can be found at Alex Kirk's [File Format Documentation Collection](http://www.schnarff.com/file-formats/).

If you are using a Linux/Unix system, you can use the [file](http://en.wikipedia.org/wiki/File_%28command%29) command to determine the file type based upon the file signature, per the system's magic file.

And, one last and final item — if you are searching for network traffic in raw binary files (e.g., RAM or unallocated space), see [Hints About Looking for Network Packet Fragments](http://www.garykessler.net/library/netsig.html).

#### ACKNOWLEDGEMENTS

The following individuals have given me updates or suggestions for this list over the years: Devon Ackerman, Nazim Aliyev, Vladimir Benko, Arvin Bhatnagar, Sam Brothers, David Burton, Alex Caithness, Björn Carlin, Per Christensson, Oscar Choi, JMJ.Conseil, Cornelis de Groot, Jeffrey Duggan, Jean-Pierre Fiset, Peter Almer Frederiksen, Tim Gardner, Chris Griffith, Linda Grody, Andis Grosšteins, Paulo Guzmán, Rich Hanes, George Harpur, Brian High, Eric Huber, Broadus Jones, Axel Kesseler, Nick Khor, Art Kocsis, Bill Kuhns, Andreas Kyrmegalos, Anand Mani, Kevin Mansell, Davyd McColl, Michal, David Millard, Bruce Modick, Lee Nelson, Dan P., Jorge Paulhiac, Carlo Politi, Stanley Rainey, Cory Redfern, Bruce Robertson, Thomas Rösner, Anli Shundi, Erik Siers, Mike Sutton, Matthias Sweertvaegher, Erik van de Burgwal, Øyvind Walding, Jason Wallace, Daniel Walton, Franklin Webber, Mike Wilkinson, Gavin Williams, and David Wright. I thank them and apologize if I have missed anyone.

I would like to give particular thanks to Danny Mares of [Mares and Company](http://www.maresware.com/), author of the [MaresWare Suite](http://www.maresware.com/maresware/software.htm%22%20%5Ct%20%22_blank) (primarily for the "subheaders" for many of the file types here), and the people at [X-Ways Forensics](http://www.x-ways.net/) for their permission to incorporate their lists of file signatures.

Finally, Dr. Nicole Beebe from The University of Texas at San Antonio posted samples of more than 32 file types at the Digital Corpora, which I used for verification and additional signatures. These files were used to develop the [Sceadan File Type Classifier](http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=06567922" \t "_blank). The file samples can be downloaded from the [Digital Corpora website](http://digitalcorpora.org/corp/nps/files/filetypes1/).

#### COPYRIGHT NOTICE

All information on this page © 2002-2015, Gary C. Kessler. Permission to use the material here is extended to any of this page's visitors, as long as appropriate attribution is provided and the information is not altered in any way without express written permission of the author.

# Additional Resources

##### A collection of useful and/or interesting material

##### Quality standards, procedures and laws.

[Forensic Science Regulator's Codes](https://www.gov.uk/government/collections/forensic-science-providers-codes-of-practice-and-conduct)

[Angus' paper on the development of the ISO/IEC 270xx standards](http://www.sciencedirect.com/science/article/pii/S1742287611000880)

[Ministry of Justice Procedure rules](http://www.justice.gov.uk/courts/procedure-rules)

[Scottish Courts & Tribunals Procedure rules](https://www.scotcourts.gov.uk/rules-and-practice/rules-of-court)

[Parliamentary Legislation Database](http://www.legislation.gov.uk/)

###### Expert Witnesses from the lawyers' perspective

"Qualifying and tendering": <https://www.youtube.com/watch?v=AZ1cyFy7hJQ>

 A law school mock trial: <https://www.youtube.com/watch?v=jweJYTCe4a8>

 How to build a cross-exam: <https://www.youtube.com/watch?v=-Kha__fMWIg>

 "Neutralising (aka tricky questions)": <https://www.youtube.com/watch?v=Ws5P2avXIQA>

[MITEC](https://www.mitec.cz/) - provider of some nice free tools, one of which is used on a couple of slides.