# Workshop 1 Computer Forensic Notes

## Familiarize with tools used for this unit:

[Autopsy (Links to an external site.)](https://www.autopsy.com/) Verify that an image is uncorrupted by comparing MD5 hash

• [FTK Imager (Links to an external site.)](https://www.exterro.com/ftk-imager)

FTK® Imager is a data preview and imaging tool that lets you quickly assess electronic evidence to determine if further analysis with a forensic tool such as Forensic Toolkit (FTK®) is warranted. Create forensic images of local hard drives, CDs and DVDs, thumb drives or other USB devices, entire folders, or individual files from various places within the media.

• [OSForensics (Links to an external site.)](https://www.osforensics.com/)•[EnCase Forensic (Links to an external site.)](https://www.guidancesoftware.com/encase-forensic) • [Oxygen Forensic Detective (Links to an external site.)](https://www.oxygen-forensic.com/en/) • [Magnet Axiom (Links to an external site.)](https://www.magnetforensics.com/)• [Registry Viewer (Links to an external site.)](https://accessdata.com/product-download/registry-viewer-1-8-0-5)  • [ExecutedProgramsList (Links to an external site.)](https://www.nirsoft.net/utils/executed_programs_list.html)  • [Aid4Mail (Links to an external site.)](https://www.aid4mail.com/) • [Wireshark](https://www.wireshark.org/)

Forensic can be use on this device.

|  |  |
| --- | --- |
| Devices | Data |
| Audio video devices | Monitor Network communication |
| Digital cameras | Timestamp, GPS location, Images data (metadata) |
| Gaming Console | Network analysis, user profile and data associated with the user profile. |
| GPS missile launcher with cameras |  |
| Digital photo frame | Metadata, Image integrity |
| Hello barbie | cloud stored data |

User profile and data associated with devices used by the users.

What data can be extracted to provide evidence of a digital crime????? Provide evidence

Operating system and platform determining the approach of forensic

Data storage can be local or in the cloud. (Data ownership)

Collecting images with Linux LinuxLeo.

Software are normally provided, licence are often costly and define use and terms.

Operating systems have different file systems and retrieving information method have to be adapted to it.

Azure lab setup

Electronics devices

Online test 🡪 file structure

Assignment 1 🡪 digital forensic plan

Assessment criteria 1 🡪 grammar, format, communication method of investigation

Assignment 2 🡪 forensic investigation plan case study

Assignment 2 = 50% / download the singles file and marge them together / See slides 29–47 of [Module 2 PowerPoint](https://courses.ecu.edu.au/courses/12665/files/1938549?wrap=1)

Assessment criteria 2 🡪 evidence is appropriate / evidences are clear with no mistakes /

Feedbacks can be requested for assignment draft

Core book system forensic investigation and response

# Questions:

How can I access to LinkedIn Learning?

# Facts

Expert testimony scientific evidence and peer review.

# Laws SRC

Criminal code act 440A unlawful use for computers

Tools SRC

Linuxleo.pdf