Digital Forensics

Michael Hegarty

Lecture 2

The Investigator's Laboratory and Tools

Objectives

- Explain how to evaluate needs for digital forensics tools
- Describe available digital forensics software tools
- List some considerations for digital forensics hardware tools
- Describe methods for validating and testing forensics tools

Understanding Forensics Lab Certification Requirements

- **Digital Forensics Lab**
  - Where you conduct your investigation
  - Store evidence
  - House your equipment, hardware, and software
- **American Society of Crime Laboratory Directors (ASCLD)** offers guidelines for:
  - Managing a lab
  - Acquiring an official certification
  - Auditing lab functions and procedures
- **ISO/IEC 27001 certified laboratory**

Determining Floor Plans for Digital Forensics Labs

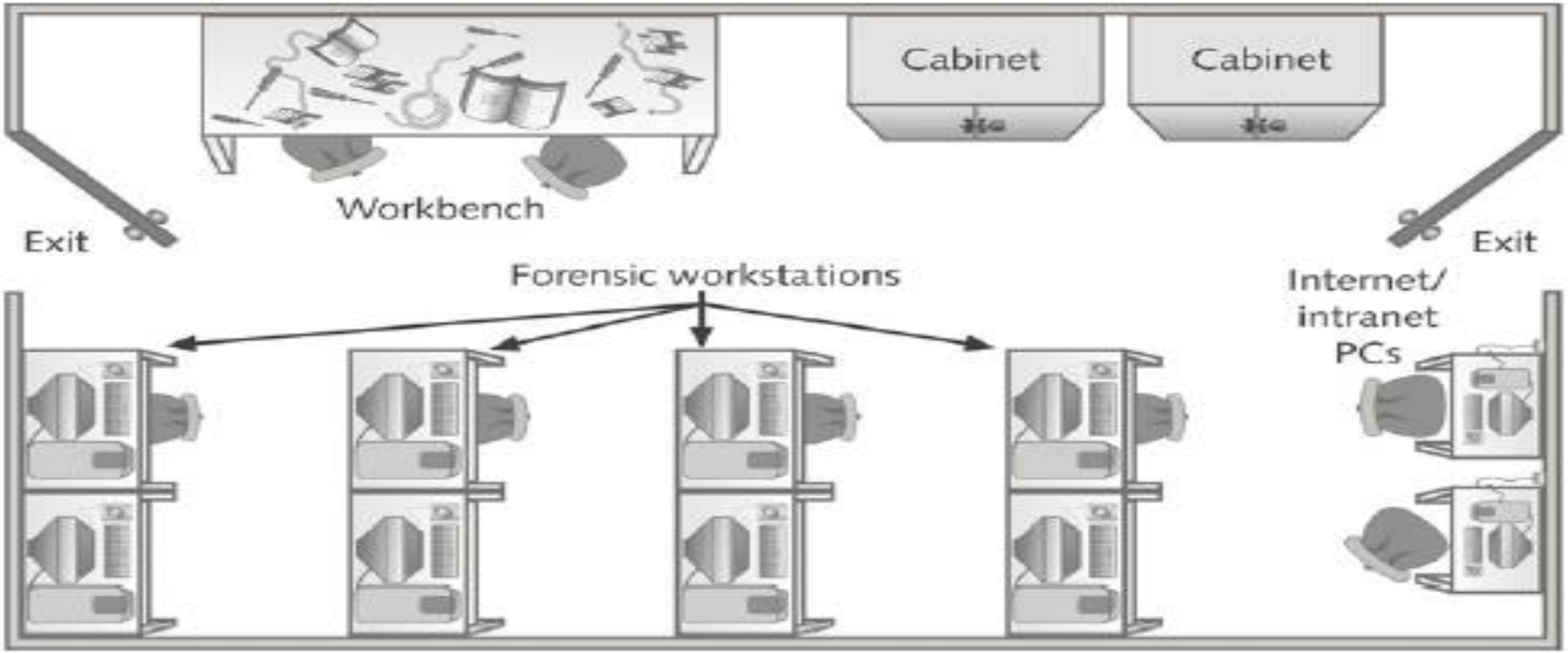


Figure 2-3 Mid-size digital forensics lab

Determining the Physical Requirements for a Computer Forensics Lab

- Most of your investigation is conducted in a lab
- Lab should be secure so evidence is not lost, corrupted, or destroyed
- Provide a safe and secure physical environment
- Keep inventory control of your assets
  - Know when to order more supplies

Maintaining Operating Systems and Software Inventories

- Maintain licensed copies of all software:
  - Microsoft Office (*current and older version*)
  - Operating Systems

- Once of Software

Planning for Equipment Upgrades

- **Risk management**
  - Involves determining how much risk is acceptable for any process or operation
  - Identify equipment your lab depends on so it can be periodically replaced
  - Identify equipment you can replace when it fails

- Computing components last 18 to 36 months under normal conditions
  - Schedule upgrades at least every 18 months
    - Preferably every 12 months

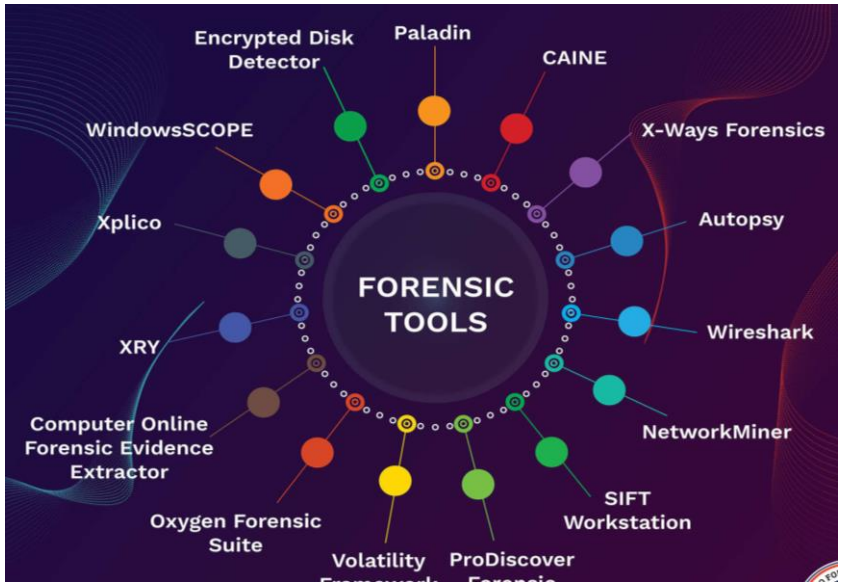
Evaluating Digital Forensics Tool Needs

- Consider open-source tools; the best value for as many features as possible

- Questions to ask when evaluating tools:
  - *On which OS does the forensics tool run*
  - *What file systems can the tool analyze?*
  - *Can a scripting language be used with the tool to automate repetitive functions?*
  - *Does it have automated features?*
  - *Is the tool validated for forensic use*

Types of Digital Forensics Tools

- Hardware forensic tools
  - Range from single-purpose components to complete computer systems and servers
- Software forensic tools
  - Types
    - Command-line applications
    - GUI applications
  - Used to copy data from a suspect's disk drive to an image file



Using a Write-Blocker

- **Write-blocker**
  - Prevents data writes to a hard disk
- Software-enabled blockers
  - Typically run in a shell mode (Windows CLI)
- Hardware options
  - Ideal for GUI forensic tools

Tasks Performed by Digital Forensics Tools

- Follow guidelines set up by NIST's Computer Forensics Tool Testing (CFTT) program
- ISO standard 27037 states: Digital Evidence First Responders (DEFRs) should use validated tools
- Five major categories:
  - Acquisition (FTK IMAGER lab-1)
  - Validation and verification
  - Extraction (ANALYSIS lab-2)
  - Reconstruction (ANALYSIS lab-2)
  - Reporting

Tasks Performed by Digital Forensics Tools

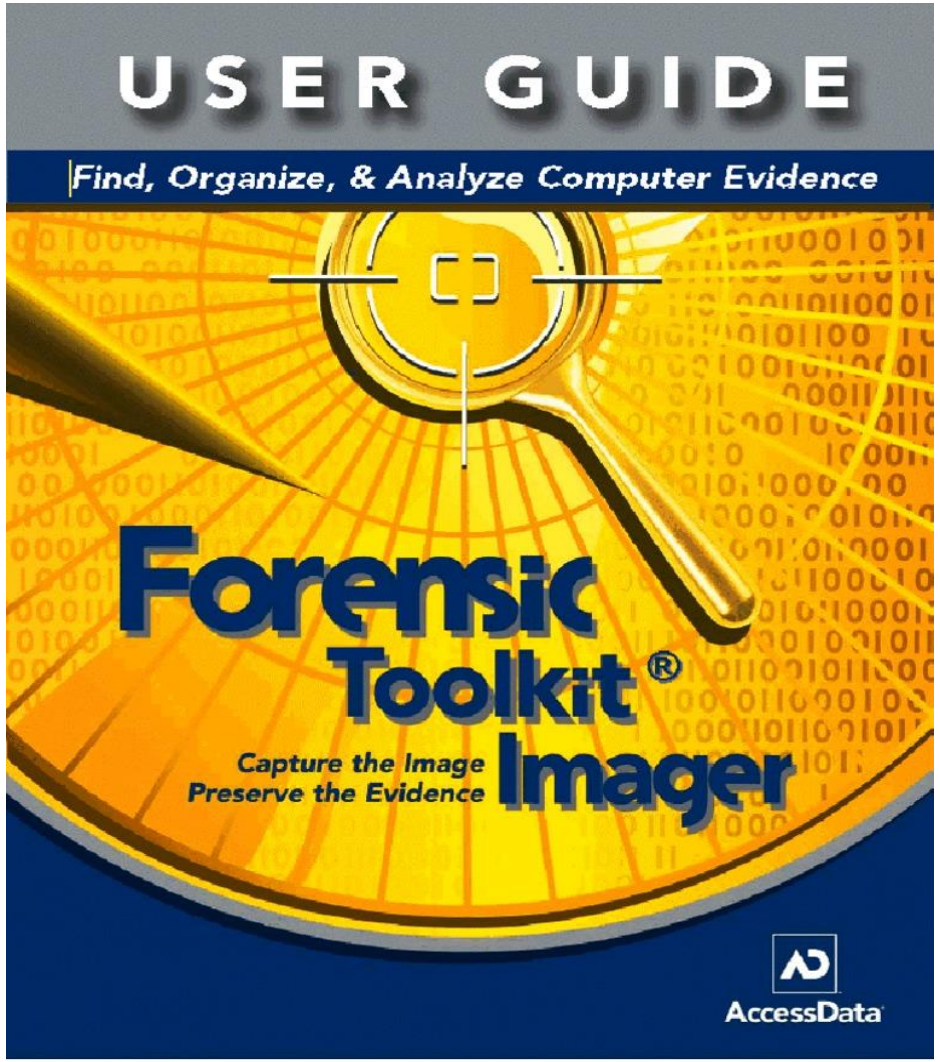
- **Acquisition**
  - Making a forensic copy of the original drive

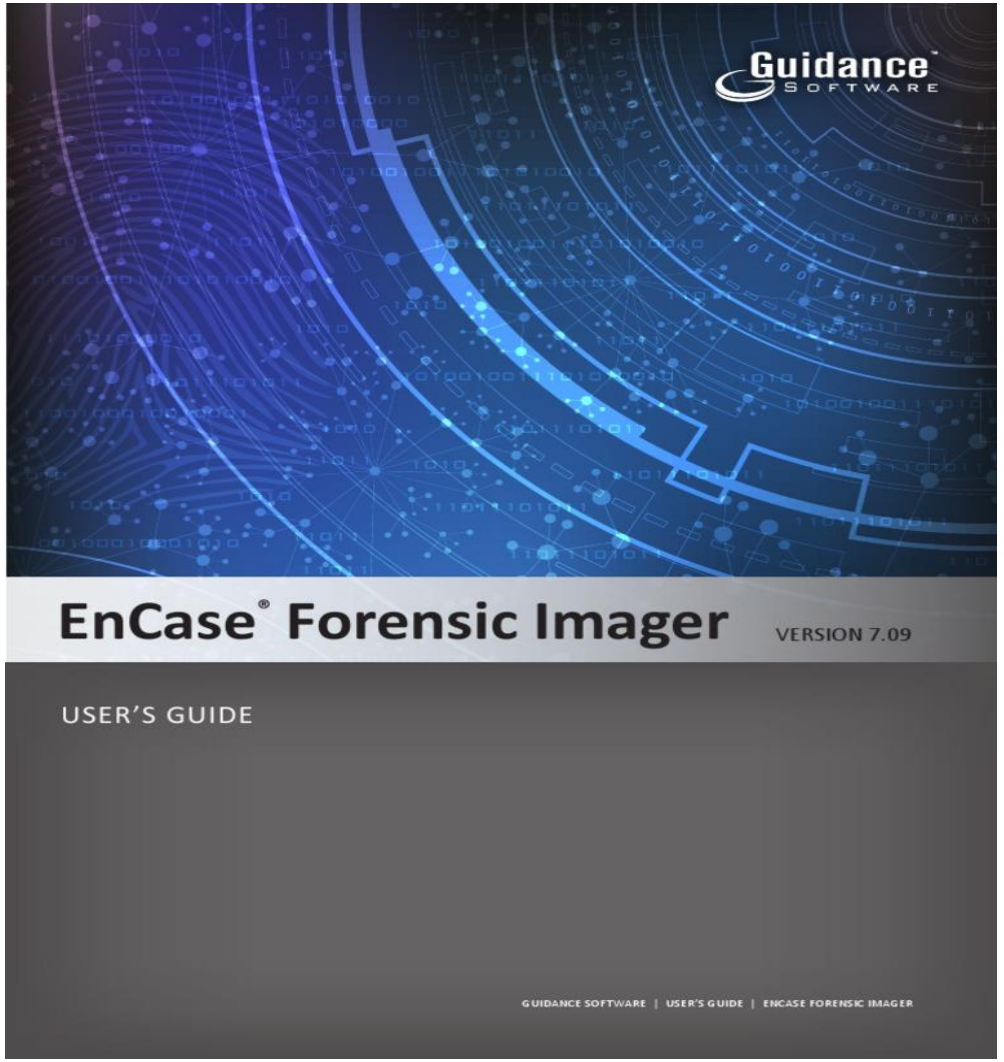
- Acquisition sub-functions:
  - Physical data copy
  - Logical data copy
  - Data acquisition format
  - Command-line acquisition
  - GUI acquisition
  - Remote, live, and memory acquisitions

Tasks Performed by Digital Forensics Tools

- Acquisition (cont'd)
  - Two types of data-copying methods are used in software acquisitions:
    - **Physical copying** of the entire drive
    - **Logical copying** of a disk partition
  - The formats for disk acquisitions vary
    - From raw data to vendor-specific proprietary
  - You can view the contents of a raw image file with any hexadecimal editor

Imager Tools





Tasks Performed by Digital Forensics Tools

- Acquisition (cont'd)
  - Creating smaller segmented files is a typical feature in vendor acquisition tools
  - Remote acquisition of files is common in larger organizations
    - Popular tools, such as FTK and EnCase, can do remote acquisitions of forensics drive images on a network

Tasks Performed by Digital Forensics Tools

- Validation and Verification
  - **Validation**
    - A way to confirm that a tool is functioning as intended
  - **Verification**
    - Proves that two sets of data are identical by calculating **hash values** or using another similar method

Tasks Performed by Digital Forensics Tools

- Validation and verification (cont'd)
  - Subfunctions
    - Hashing

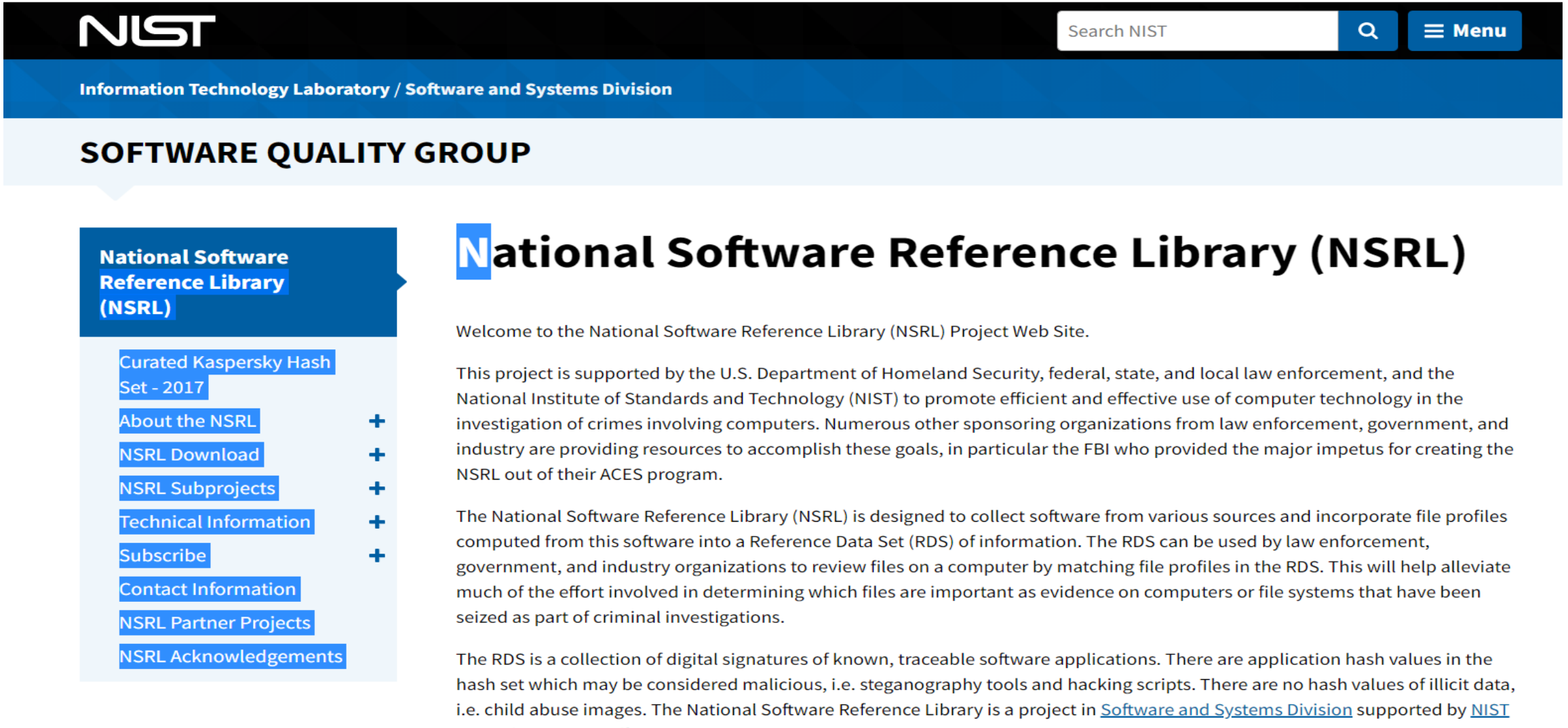
      MD5, SHA (Secure Hash Algorithms)
    - Analyzing file headers
      - Discriminate files based on their types
  - National Software Reference Library (NSRL) has compiled a list of known file hashes
    - For a variety of OSs, applications, and images

https://www.nist.gov/itl/ssd/software-quality-group/national-software-reference-library-nsrl

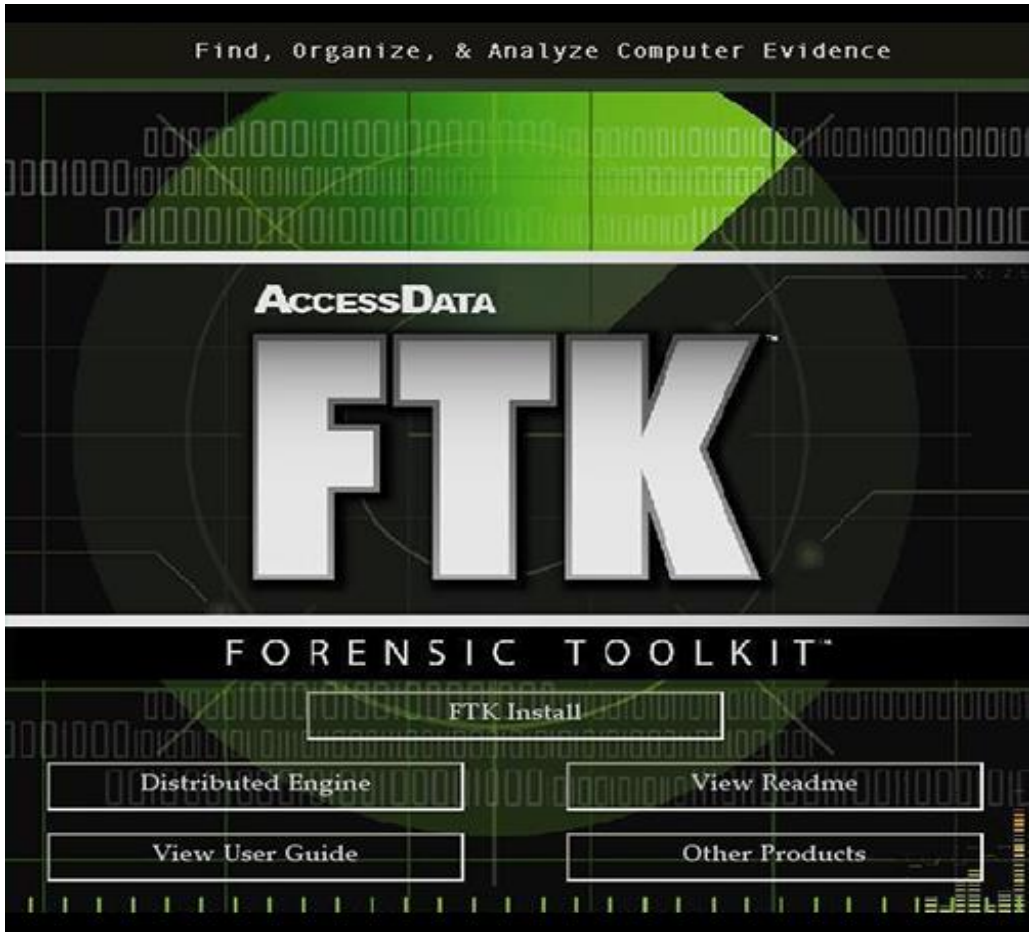
Hash Function

- Creates a “fingerprint” identification code so that it can be compared to another copy of the file / data to determine if it has been altered.
- Used to verify integrity of evidence as exactly matching original
- Can use either MD5 or SHA algorithms
- Can hash a single file or multiples or entire disk
- Most forensics software has built-in hashing utilities

Tasks Performed by Digital Forensics Tools



Digital Forensics Tools



Tasks Performed by Digital Forensics Tools

- **Extraction**
  - Recovery task in a digital investigation
  - Most challenging of all tasks to master
  - Recovering data is the first step in analyzing an investigation's data
  - Lab 2 Analysis

Tasks Performed by Digital Forensics Tools

- Extraction (cont'd)
  - From an investigation perspective, encrypted files and systems are a problem
  - Many password recovery tools have a feature for generating potential password lists
    - For a **password dictionary attack**
  - If a password dictionary attack fails, you can run a **brute-force attack**

Tasks Performed by Digital Forensics Tools

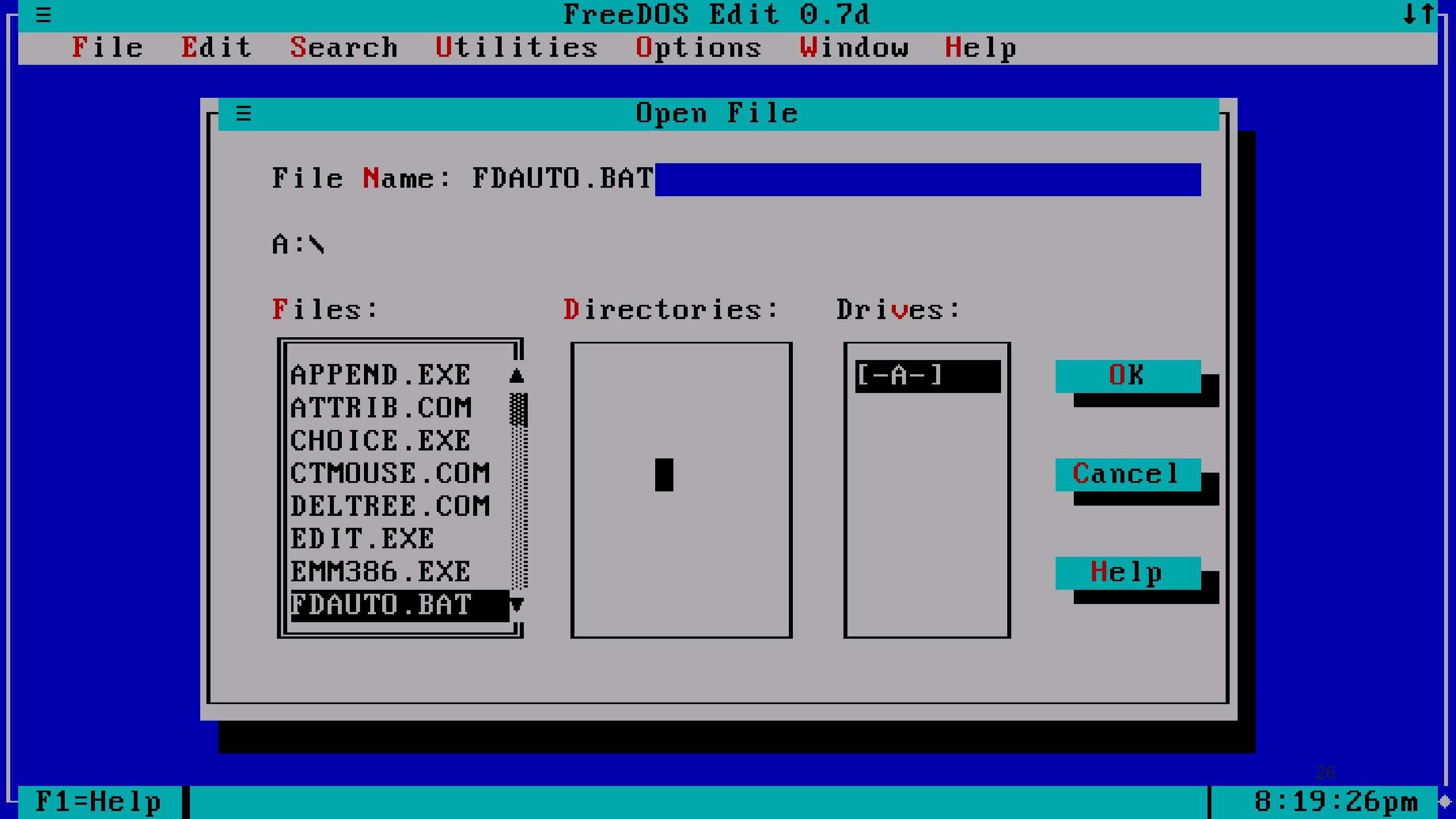
- Reconstruction (cont'd)
  - To re-create an image of a suspect drive
    - Copy an image to another location, such as a partition, a physical disk, or a virtual machine
    - Simplest method is to use a tool that makes a direct disk-to-image copy
  - Examples of disk-to-image copy tools:
    - FTK Imager
    - Linux dd command
    - ProDiscover

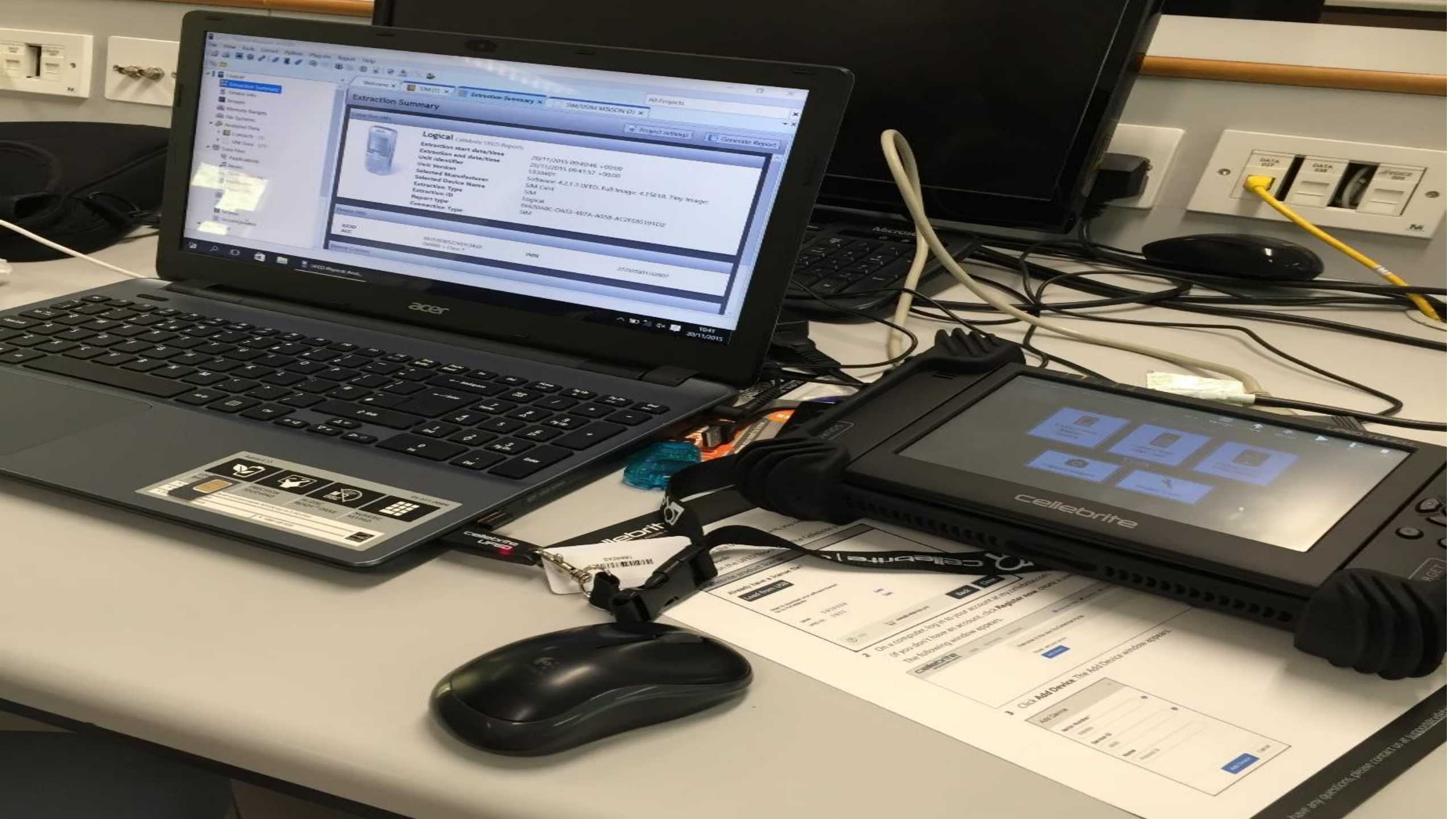
Tasks Performed by Digital Forensics Tools

- Reporting
  - To perform a forensics disk analysis and examination, you need to create a report
  - Subfunctions of reporting
    - Bookmarking or tagging
    - Log reports
    - Report generator
  - Use this information when producing a final report for your investigation

Digital Forensics Software Tools

- The following sections explore some options for command-line and GUI tools in both Windows and Linux


FreeDOS Edit 0.7d
File Edit Search Utilities Options Window Help
Open File
File Name: FDAUTO.BAT
A:\
Files:
Directories:
Drives:
APPEND.EXE
ATTRIB.COM
CHOICE.EXE
CTMOUSE.COM
DELTREE.COM
EDIT.EXE
EMM386.EXE
FDAUTO.BAT
[-A-]
OK
Cancel
Help
F1=Help
8:19:26pm


Extraction Summary
Logical
acer
cellebrite

Linux Forensics Tools

- Kali Linux
  - Formerly known as BackTrack
  - Includes a variety of tools and has an easy-to-use KDE interface


KALI LINUX™
“the quieter you become, the more you are able to hear”

Linux Forensics Tools

- **Autopsy**
  - Sleuth Kit is a Linux forensics tool
  - Autopsy is the GUI browser interface used to access Sleuth Kit's tools
  - **FREE**
  - **https://www.autopsy.com/**

SANTOKU

INFO
About Santoku

HOWTO'S
Slice, dice and mince

COMMUNITY
Join the discussion

DOWNLOAD
Get it now, free

Santoku 0.5 – Packaged & Delivered

To make future updating of Santoku WAY easier for users, we're hosting a repository. Set it up just once and get updates with package management instead of downloading a whole new iso.

DOWNLOAD

Santoku is free and Open Source.

The word santoku loosely translates as 'three virtues' or 'three uses'. Santoku Linux has been crafted to support you in three endeavours:

Mobile Forensics

Tools to acquire and analyze data

- Firmware flashing tools for multiple manufacturers
- Imaging tools for NAND, media cards, and RAM
- Free versions of some commercial forensics tools
- Useful scripts and utilities specifically designed for mobile forensics

Mobile Malware

Tools for examining mobile malware

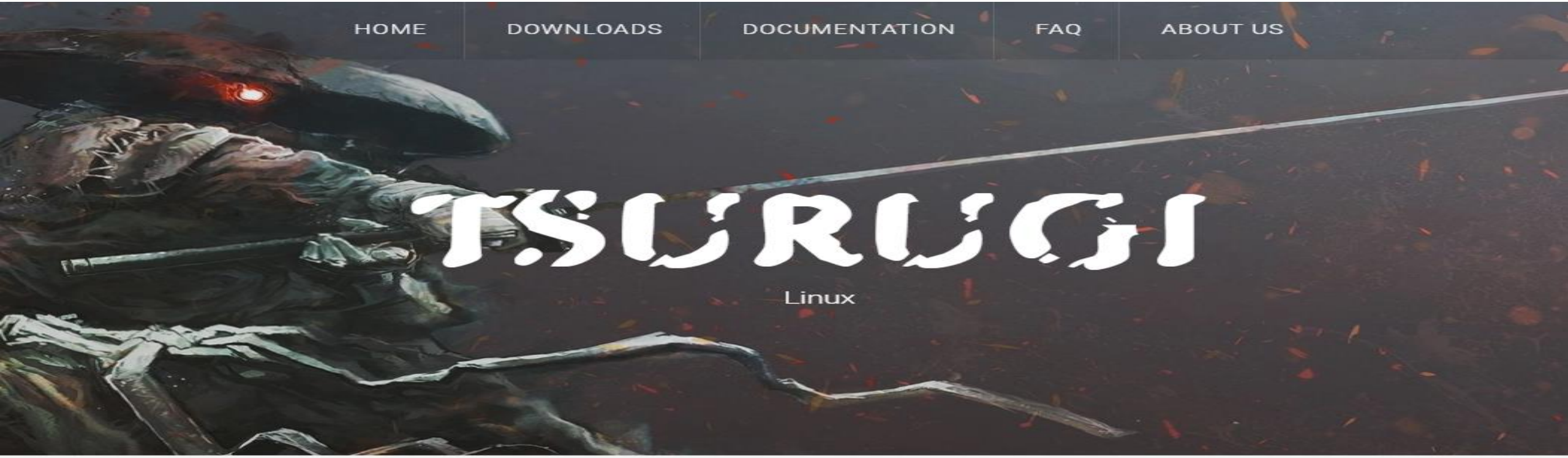
- Mobile device emulators
- Utilities to simulate network services for dynamic analysis
- Decompilation and disassembly tools
- Access to malware databases

Mobile Security

Assessment of mobile apps

- Decompilation and disassembly tools
- Scripts to detect common issues in mobile applications
- Scripts to automate decrypting binaries, deploying apps, enumerating app details, and more

https://tsurugi-linux.org/



Your DFIR Linux distribution

Tsurugi Linux is a DFIR open source project that is and will be totally free, independent, without involving any commercial brand
Our main goal is share knowledge and "give back to the community"

A Tsurugi (剣) is a legendary Japanese double-bladed sword used by ancient Japan monks

https://csilinux.com/download

Download CSI Linux

2022.1.1 has been released!

Default username: csi | Default password: csi

Brief overview

CSI Linux has been completely rebuilt using Ubuntu 22.04 LTS server and the backend operating system. CSI Linux has many updated tools, features, and additions. To install CSI Linux Tools updates type "powerup" in the terminal window and press enter. This will not only keep the OS up to date, but also third party tools and out proprietary CSI Tools.

When turned on, the CSI_TorVPN encapsulates all traffic through Tor similar to how Tails works. The CSI_Gateway app is now pointing to at a Whonix gateway VM. This gives you two different options when using the Virtual Appliance. If you are using the bootable version, you can only use the CSI_TorVPN.

You can also add a VPN or Tor gateway to your network router for an external network layer of security.

The CSI Linux SIEM has been separated and is now separate from CSI Linux. Elasticsearch, Kibana, Logstash, Zeek, and others have been combined into this growing network monitoring and forensic server environment. This will be able to be downloaded onto CSI Linux or used on another system on the network.

Stay in touch with CSI Linux

SUBSCRIBE TO NEWSLETTER

GUI Forensics Tools

- GUI forensics tools can simplify digital forensics investigations
- Have also simplified training for beginning examiners
- Most of them are put together as suites of tools
- Advantages
  - Ease of use
  - Multitasking
  - No need for learning older OSs

GUI Forensics Tools

- Disadvantages
  - Excessive resource requirements
  - Produce inconsistent results
  - **Create tool dependencies**
    - Investigators' may want to use only one tool
    - Should be familiar with more than one type of tool

4 types of disk duplication

- *Simple file copying* – misses some files (in use) and changes timestamps
- *Advanced file copying* – can copy systems files and deleted files, used in restoring and recovering files
- *Partition duplication* – grabs entire partition e.g. symantec ghost
- **Forensic duplication – can copy Slack and Unallocated space**
  - **Slack Space** is unused space in a cluster
    - Old file information can be recovered from slack space
  - **Unallocated Space** is space marked as free after a file is deleted
    - Space is not overwritten, only marked as free
    - Need utility to extract deleted files

Bit-stream Images

- High quality copies – most useful
- Process to produce forensically sound duplicates or images
- Acquires media bit by bit (literally)
- Images can be analysed and data “carved” from them regardless of deletion state

Validating and Testing Forensic Software

- *Evidence could be admitted in court*

- National Institute of Standards and Technology (NIST)
- National Software Reference Library (NSRL) project
  - Collects all known hash values for commercial software applications and OS files
  - *https://www.nist.gov/itl/ssd/software-quality-group/national-software-reference-library-nsrl/about-nsrl/nsrl-introduction*
- Computer Forensics Tool Testing (CFTT)
  - Project to manage research on forensic tool testing
  - *https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt*

Using National Institute of Standards and Technology Tools

- NIST publishes articles, provides tools, and creates procedures for testing/validating forensics software

- Computer Forensics Tool Testing (CFTT) project
  - Manages research on computer forensics tools

- NIST has created criteria for testing computer forensics tools based on:
  - Standard testing methods
  - ISO 17025 criteria for testing items that have no current standards

Using Validation Protocols

- Always verify your results by performing the same tasks with other similar forensics tools

- Use at least two tools
  - Retrieving and examination
  - Verification

- **Understand how forensics tools work**

Summary

- Consult your business plan to get the best hardware and software
- Computer forensics tools functions
  - Acquisition
  - Validation and verification
  - Extraction
  - Reconstruction
  - Reporting
- Maintain a software library on your lab

Summary

- Computer Forensics tools types
  - Software
  - Hardware
- Forensics software
  - Command-line
  - GUI
- Forensics hardware
  - Customized equipment
  - Commercial options
  - Include workstations and write-blockers

Summary

- Tools that run in Windows and other GUI environments don't require the same level of computing expertise as command-line tools
- Always run a validation test when upgrading your forensics tools
- THANK YOU!