Co-funded by the Erasmus+ Programme of the European Union

ISSES

ISSES – Information Security Services Education in Serbia

Supported by the Erasmus+ Capacity Building in the field of Higher Education (CBHE) grant N° 586474-EPP-1-2017-1-RS-EPPKA2-CBHE-JP

Digital Forensics Laboratory Design

Version 1.0

Author(s)/Organisation(s):
Stevan Gostojić / UNS-FTN Bratislav Predić, Dragan Stojanović / UNI Bojan Jovanović, Dejan Simić / UB-FON

Date of final release:
April 10th, 2020
Relevant Work Package(s):
WP3 – Lab development
Short Description:
A specification of Digital Forensics Laboratory design.
Keywords:
digital forensics, laboratory

Revision History:				
Revision	Date	Author(s)	Status	Description
0.1	Apr 6, 2020	Stevan Gostojić	working draft	Initial draft.
1.0	Apr 10, 2020	Stevan Gostojić, Bratislav Predić, Bojan Jovanović	Release	

CONTENTS

Co-funded by the Erasmus+ Programme of the European Union

ISSES

ISSES – Information Security Services Education in Serbia

Supported by the Erasmus+ Capacity Building in the field of Higher Education (CBHE) grant N° 586474-EPP-1-2017-1-RS-EPPKA2-CBHE-JP

Supported by the Erasmus+ Capacity Building in the field of Higher Education (CBHE) grant N° 586474-EPP-1-2017-1-RS-EPPKA2-CBHE-JP

1 Introduction

This document specifies digital forensics laboratory design by describing the laboratory setup and the equipment specification.

The laboratory setup includes the description of the setup of several specialized digital forensics stations. Every digital forensics laboratory can choose which digital forensics stations it will develop to satisfy its unique needs.

The equipment specification includes specification of hardware, software, test datasets, and consumables. Hardware includes both general purpose hardware (e.g. computers, monitors, digital cameras, digital voice recorders, etc.) and specialized hardware (e.g. forensic bridges, forensic duplicators, mobile acquisition devices, etc.) and software includes both commercial and open-source digital forensics software.

2 Setup

A digital forensic laboratory can have several specialized digital forensics stations: a computer acquisition station, a mobile device acquisition station, a hardware acquisition station, a forensics analysis station, a cryptanalysis station, and a field acquisition station. Also, the laboratory should have a storage space to store digital evidence, tools, and consumables.

Also, each laboratory can choose to use either commercial digital forensics software tools, open-source digital forensics software tools, or combination thereof. The first category of software tools is usually easier to use and offers more functions, while the second category is usually more affordable.

Depending on the laboratory's resources and unique needs, every laboratory will develop the stations that best fulfil those needs with available resources.

2.1 Computer Acquisition Station

The computer acquisition station is used to acquire digital evidence from "classic" computers such as desktop or laptop computers.

It consists of: a forensic bridge (#1.1), a desktop computer (#2.1), a computer monitor (#2.2), and a computer repair kit (#1.3). Depending on the decision made, it can use either commercial (#3.2) or open-source (#4.2) digital forensics computer acquisition tools.

2.2 Mobile Device Acquisition Station

The mobile device acquisition station is used to acquire digital evidence from mobile devices such as mobile phones and tablets.

It consists of: a mobile device acquisition device (#1.4) and a mobile device repair kit (#1.5). It uses a commercial (#3.3) digital forensics mobile device acquisition tools.

2.3 Hardware Acquisition Station

The hardware acquisition station is used to acquire data directly from memory chips. Three most popular techniques are JTAG, ISP, or chip-off. This methods are usually necessary to acquire digital evidence from either latest generation of mobile devices or embedded devices.

It consists of: a JTAG acquisition device (#1.6 and/or #1.7), a desktop computer (#2.1), a computer monitor (#2.2), a computer repair kit (#1.3), and a mobile device repair kit (#1.5).

2.4 Forensics Analysis Station

The forensics analysis station is used to analyse the digital evidence and write the report presenting the evidence to the interested parties (e.g. law enforcement, courts of law, or companies).

It consists of: a desktop computer (#2.1) and a computer monitor (#2.2).

Depending on the decision made, it can use either commercial (#3.2) or open-source (#4.2, #4.3 and #4.4) digital forensics analysis tools.

This station also includes appropriate training datasets such as disk images (#5.1), memory dumps (#5.2), and network traces (#5.3).

2.5 Cryptanalysis Station

The cryptanalysis station is used to decrypt encrypted data, such as office documents, e-mails, or files in general, when no encryption keys are available.

It consists of: a cryptanalysis device (#1.8), a desktop computer (#2.1), and a computer monitor (#2.2).

This station also includes appropriate training datasets such as disk images (#5.1), memory dumps (#5.2), and network traces (#5.3).

2.6 Field Acquisition Station

The field acquisition station is used to acquire digital evidence in the field. For the purpose of educating students, a small “crime scene” will be simulated by equipping a “dummy” workplace.

It consists of: a forensic duplicator (#1.2), a computer repair kit (#1.3), a mobile device acquisition device (#1.4), a mobile device repair kit (#1.5), a laptop computer (#2.3), a digital camera (#2.4), a camera bag (#2.5), and a digital voice recorder (#2.6).

Depending on the decision made, it can use either commercial (#3.2) or open-source (#4.2) digital forensics computer acquisition tools. It also uses a commercial (#3.3) digital forensics mobile device acquisition tools.

2.7 Storage Space

The storage space is used to (securely) store digital evidence as well as the tools and consumables necessary for the digital forensic process.

3 Hardware Specification

This section specifies the hardware needed to develop a digital forensics laboratory. It is divided into specialised digital forensics hardware specification and general-purpose hardware specification.

The specialized digital forensics hardware is specified in Table 1.

Table 1: Specialized hardware.

No.	Name	Description
1.1	Forensic Bridge	Connectors: Host Side (Rear) Data: One USB 3.0 Standard-B connector DC Input: Two SATA 15-pin (male) connectors for input DC power Connectors: Device, Write-Blocked (Front Panel) PCIe: One PCIe custom data + power connector (for Tableau PCIe cable) SATA/SAS: One SATA/SAS data connector (SAS Gen. 1, SATA Gen. 2) SATA: One SATA (Gen. 3) data connector USB 3.0: One USB 3.0 Standard-A connector FireWire: One FireWire800 9-pin connector IDE: One IDE signal connector DC Out: One DC Out 3M 4-pin drive power connector (for IDE, SAS, SATA & PCIe) Physical Power: 9.5 watts typical operating (not including attached storage devices) Supply Voltage (DC IN): +5V @ 1.65A (min), +12V @ 0.1A (min) Output Voltage (DC OUT): +5VDC @ 2A, +12VDC @2A Relative Humidity: Up to 90% (non-condensing) Operating Temperature Range: 0 to 55 degrees C (no airflow) Storage Temperature Range: -20 to 60 degrees C Dimensions: 5.875 in. (L) x 5.75 in. (W) x 1.625 in. (H) Weight: 11.2oz (320g)
1.2	Forensic Duplicator	Connectors: Source Side SATA/SAS: Two SATA/SAS (6 Gbps) Signal Connectors USB: One USB 3.1 Gen 1 (5 Gbps) Standard-A Connector FireWire: One 1394b "FireWire800" Signal Connector PCIe: One PCIe (10 Gbps) Adapter Connector

		Drive Power: Two 3M-style 4-pin Power Connectors for the SATA/SAS Drive Power Connectors: Destination Side SATA/SAS: Two SATA/SAS (6 Gbps) Signal Connectors USB: One USB 3.1 Gen 1 (5 Gbps) Standard-A Connector TX1-S1: One TX1-S1 (Two SATA/SAS 6 Gbps) Signal Connector Drive Power: Two 3M-style 4-pin Power Connectors for the SATA/SAS Drive Power Connectors: Misc Ethernet: One 10 Gbps Ethernet Connection (Source or Destination) USB: Two USB 3.1 Gen 1 (5 Gbps) Standard-A Connectors SD Card: One SD Card Connector for Device Firmware DC Input: One Barrel Connector for use with Tableau TP6 Power Supply Physical Power: 55 Watts Typical Operating (Not Including Drive Power) DC Input: 24 VDC (Nominal) DC Output: (per drive): +5/12V @2A (Spin-up) +5/12V @1A (Continuous) Dimensions: 9.5 in. (L) x 6.5 in. (W) x 2.625 in. (H) Weight: 35 oz (980 g) Storage Temperature Range: -20 to 70 Degrees C Operating Temperature Range: 0 to 40 Degrees C Ambient (Room Temperature) Relative Humidity: Up to 90% (Non-condensing) Add Ons IDE Adapter PCIe Adapters bundle Adapters for older drive designs
1.3	Computer Repair Kit	1 x Slotted screwdriver - #0 1 x Slotted screwdriver - #1 1 x Slotted screwdriver - #2 1 x Slotted screwdriver - 1/4" 1 x Slotted screwdriver - 1/8" 1 x Slotted screwdriver - 3/16" 1 x Reversible T10/T15 Torx screwdriver 1 x Nut driver - 1/4" 1 x Nut driver - 3/16" 1 x 5-1/2" long nose plier

		1 x 6" adjustable wrench 1 x 8" wire cutter/stripper 1 x Three prong parts retriever 1 x 4-1/2" Needle Nose Tweezer 1 x Assembly tweezers 1 x Chip extractor 1 x Chip inserter with pin straightener 1 x CSA approved soldering iron and solder 1 x Spare Parts Container 1 x Anti-static Wrist Strap 1 x Anti-static Mat 1 x Storage Case
1.4	Mobile Device Acquisition Device	Mobile Device Logical and Physical Examinations Tablet & GPS Devices Examinations Memory Card Logical and Physical Examinations SIM Card Reading and Cloning Secure XRY file with forensic log Hash Algorithms File Signature Analysis Selective Extraction of Data
1.5	Mobile Device Repair Kit	2 x Spudger tools 1 x Triangle pry-tool 1 x Set of tweezers 1 x Multi-bit screwdriver 5 x Torx bits (T4, T5, T6, T8, T10) 4 x Phillips bits (PH000, PH00, PH0, PH1) 3 x Pentalobe bits (P2, P5, P6) 2 x Tri-wing bits (TRI0, TRI1) 1 x Slot bit (2.0) 1 x Hex bit (2 mm) 1 x Suction cup 1 x SIM card ejector pin 1 x Anti-static wrist strap 1 x Anti-static mat 1 x Atorage case
1.6	JTAG Acquisition Device	0-5.5volt tolerant pins 0-6volt measurement probe 1Hz-40MHz frequency measurement 1kHz - 4MHz pulse-width modulator, frequency generator On-board multi-voltage pull-up resistors

		On-board 3.3volt and 5volt power supplies with software reset Macros for common operations Bus traffic sniffers (SPI, I2C) A bootloader for easy firmware updates Transparent USB->serial mode 10Hz-1MHz low-speed logic analyzer Servo driver Can program many AVR microcontrollers Supported by AVRdude Can emulate the AVR STK500 v2 with alternate ST500 Clone firmware Programs FPGAs and CPLDs with alternate XSVF firmware Scriptable from Perl, Python, etc.
1.7	JTAG Acquisition Device	Interfacing with embedded devices, debugging them, bit-banging, fuzzing, etc. via USB to a number of different low-level data interfaces including: JTAG, SPI, I2C, UART and GPIO.
1.8	Cryptanalysis Device	Server Case: 2U chassis - Includes standard 26 in. sliding rail kit CPU: Intel Xeon ES-1620 Quad Core Acceleration: Four Tableau Accelerator Version 2 FPGA-based Cards (TACC2) Memory: 16GB ECC DDR4 RAM Storage: 256 GB SSD On-Board Display: 5 in. LCD Power Supply: 460W Ethernet: Dual-port GbE NIC Operating System: Microsoft Windows 10 x64 Included Software: Passware Decryption Server, Passware Kit Agent or Passware Kit Forensic

The general-purpose hardware is specified in Table 2.

Table 2: General-purpose hardware.

No.	**Name**	**Description**
2.1	Desktop Computer	Processor: Intel Core i7-7700 Processor (8MB Cache, up to 4.20GHz) Operating System: Windows 10 Pro 64 Memory: 16GB DDR4 2400 UDIMM Graphics: NVIDIA Geforce GT730 2GB DDR5 64bit DP High Profile

No.	Name	Description
		Storage: 2 x 2TB Hard Drive, 7200 RPM, 3.5", SATA + 1 x 512GB PCIe Solid State Drive Optical Drive: Slim DVD Burner / CD-RW, SATA Networking: Integrated Intel Gigabit Ethernet Form Factor: Tower Power 600W, at least 2 x 5.25” half-height drive bays
2.2	Computer Monitor	Maximum Resolution: 2560 x 1440 Connections: DP 1.2, HDMI 1.4 Display Type: IPS Brightness: 350 cd/m2 Aspect Ratio: 16:9 Stand: Lift, Tilt, Swivel, Pivot Refresh Time: 6 ms Screen Illumination: LED Backlight Contrast Ratio: 1000:1 Viewable Image Size Inches: 27
2.3	Laptop Computer	Processor: 2.2-GHz Intel Core i7-8750H OS: Windows 10 Pro RAM: 32GB SSD: 1TB GPU: GTX1050 Monitor: UHD touch (Dell XPS 15 9560 или сличан лаптоп)
2.4	Digital Camera	Tripod socket: 1/4–in. (ISO 1222) Wi-Fi (Wireless LAN) range (line of sight): Approximately 10 m (32 ft) without interference; range may vary with signal strength and presence or absence of obstacles Viewfinder: Eye-level pentamirror single-lens reflex viewfinder Storage file formats: NEF (RAW): 12- or 14 bit, compressed, JPEG: JPEG-Baseline compliant with fine (approx. 1 : 4), normal (approx. 1 : 8), or basic (approx. 1 : 16) compression, NEF (RAW)+JPEG: Single photograph recorded in both NEF (RAW) and JPEG formats Flash sync speed: X = 1/200 s; synchronizes with shutter at 1/200 s or slower

No.	Name	Description
		Lens servo: Single-servo AF (AF-S), Continuous-servo AF (AF-C), Auto AF-S/AF-C selection (AF-A); predictive focus tracking activated automatically according to subject status, Manual focus (MF): Electronic rangefinder can be used Focus points: 39, can be selected from 39 or 11 focus points Flash modes: Auto, auto with red-eye reduction, auto slow sync, auto slow sync with red-eye reduction, fill-flash, red-eye reduction, slow sync, slow sync with red-eye reduction, rear-curtain with slow sync, rear-curtain sync, off Battery: One EN-EL14a rechargeable Li-ion battery Storage media: SD, SDHC (UHS-I compliant), SDXC (UHS-I compliant) Total pixels: 24.78 million
2.5	Camera Bag	Weight: 0.3 kg or less External Dimensions: 18 x 12.6 x 19.1 cm or less Internal Dimensions: 17.3 x 11 x 17 cm Front Compartment Dimensions: 15 x 1 x 13.2 cm Main Color: Black
2.6	Digital Voice Recorder	Headphone Connector: 3.5 mm USB: High-speed USB 2.0 Connector Screen Type: LCD Color Display Screen Resolution: 128 × 160 pixels Screen Diagonal: 1.77"/4.5 cm Memory: 8 GB NAND Flash Mic: HQ Stereo, Low-Noise Sensitivity Formats: MPEG1 layer 3 (MP3), PCM (WAV) Modulations: PCM 1411 kbps,SHQ 192 kbps,HQ 96 kbps,SP 64 kbps,LP 8 kbps Sample Rate: 44,1 kHz (PCM/SHQ), 32 kHz (HQ), 22 kHz (SP), 16 kHz (LP) Bit Rate: 8, 64, 96, 192, 1411 kbps Recording Time: 2280 h (LP), 284 h (SP), 190 h (HQ), 90 h (SHQ), 12 h (PCM) Sound Frequency Range: 50 – 20000 Hz

No.	Name	Description
		Speaker Output Power: 110 mW Speaker Diameter: 28 mm Batteries: AAA/LR03 Alkaline - 50/25 h in LP Record Mode OS: Windows 10/8/7, macOS 10, Linux Dimensions: 4.5 x 11.3 x 2 cm Weight: 79 g

Co-funded by the Erasmus+ Programme of the European Union

ISSES

ISSES – Information Security Services Education in Serbia

Supported by the Erasmus+ Capacity Building in the field of Higher Education (CBHE) grant N° 586474-EPP-1-2017-1-RS-EPPKA2-CBHE-JP

4 **Software** Specification

This section specifies the software needed to develop a digital forensics laboratory. It is divided into commercial digital forensics software specification and open-source digital forensics software specification.

The commercial software is specified in Table 3.

Table 3: Commercial software.

No.	Name	Description
3.1	Operating System	Microsoft Windows 10
3.2	Disk Analysis Tool	AccessData Forensic Toolkit (FTK)
3.3	Mobile Device Analysis Tool	MSAB Office

The open source software is specified in Table 4.

Table 4: Open-source software.

No.	Name	Description
4.1	Operating System	Kali Linux or Ubuntu
4.2	Disk Analysis Tool	The Sleuth Kit + Autopsy
4.3	Memory Analysis Tool	Volatility
4.4	Network Analysis Tool	Wireshark

5 Datasets Specification

This section specifies the digital forensics training datasets. They are to be used to train students in the analysis phase of a digital forensics investigation.

The training datasets are specified in Table 5.

Table 5: Training datasets.

No.	**Name**	**Description**
5.1	Disk Images	Disk images for computer and mobile forensics analysis training.
5.2	Memory Dumps	Memory dumps for computer and mobile forensics training.
5.3	Network Traces	Network traces for network forensics training.

6 **Consumables** Specification

This section specifies the consumables found in the digital forensics laboraotry.

The consumables are specified in Table 6.

Table 6: Consumables.

No.	**Name**	**Description**
6.1	Desktop Computer	A used desktop computer used for computer data acquisition training.
6.2	Laptop Computer	A used laptop computer used for computer data acquisition training.
6.3	Cell Phone	A used cell phone used for mobile device data acquisition training.
6.4	SATA HDD	Internal, 3.5’’, SATA, 1TB, 7200 RPM
6.5	USB HDD	External, 2.5’’, USB 3.1, 1TB
6.6	PCIe SDD	M.2 2280, PCIe, 512GB, 3D NAND
6.7	SD Card	microSD, SD adapter, 64GB, 10 U3
6.8	USB Thumb Drive	USB 3.1, 128GB, 15 MB/s write speed, 110 MB/s read speed
6.9	Storage boxes	n/a
6.10	Antistatic bags	n/a
6.11	Labels	n/a