Deliverable D2.6

Analysis and Acquisition of Teaching and Learning Resources

Author(s):	Charles Daly, Darragh O'Brien, Renaat Verbruggen
Editor(s):	
Responsible Organization:	Dublin City University
Version-Status:	1.0
Submission date:	2019 February 25
Dissemination level:	Project

Deliverable factsheet

Project Number:	**574063-EPP-1-2016-1-IT-EPPKA2-CBHE-JP**
Project Acronym:	FORC
Project Title:	Pathway in Forensic Computing

Title of Deliverable:	**Analysis and Acquisition of Teaching and Learning Resources (D2.6)**
Work package:	WP2
Due date according to contract:	2018-06-30

Editor(s):	Renaat Verbruggen
Contributor(s):	Charles Daly, Darragh O'Brien,
Reviewer(s):	
Approved by:	

Abstract:	This document brings together the Teaching and Learning Resources used across all the modules that are being developed in the Project.
Keyword List:	Teaching resources

Consortium

	Role	*Name*	*Short Name*	*Country*
1.	Coordinator, academic partner	The University of Cagliari	UniCA	Italy
2.	Forensic Computing Education expert, academic partner	Middlesex University	MU	United Kingdom
3.	Forensic Computing Education expert, academic partner	Dublin City University	DCU	Ireland
4.	Academic partner to establish a pathway program in forensic computing	Al-Quds university	AQU	Palestine
5.	Academic partner to establish a pathway program in forensic computing	Palestine Technical University, Kadoorie	PTUK	Palestine
6.	IT and forensic software developer partner	Al-Andalus Software Development	ASD	Palestine
7.	Academic partner to establish a pathway program in forensic computing	Princess Sumaya University for Technology,	PSUT	Jordan
8.	Academic partner to establish a pathway program in forensic computing	The University of Jordan	JU	Jordan

Revision History

Version	*Date*	*Revised by*	*Reason*
V1.0	31-01-2019	Charles Daly, Darragh O'Brien, Renaat Verbruggen	Original document based on information provided by partners.

Table of Contents

List of Figures

No Figures included

List of Tables

No tables included

List of Abbreviations

The following table presents the capitalizations used in the deliverable in order of use.

Abbreviation	*Description*
WP	Work Package
WPL	Work Package Leader
FORC	Pathway in Forensic Computing
ICT	Information Communication Technology
PS	Palestine
JO	Jordan

1. Document overview

The following are the listed teaching and learning resources for each of the modules that are being developed within the project. Partners within the consortium have reviewed these module descriptions and the final revised versions are given here.

Title	Primary Creator
1. Foundations of Digital Forensics	AQU
2. Digital Forensic Procedures	AQU
3. Legal aspects of Digital Forensics	JU
4. Business aspects of Digital Forensics and Ethics	JU
5. Digital Investigation Tools and Techniques	PTUK
6. Network forensics	PSUT
7. Mobile Forensics	PSUT
8. Emerging Trends and special topics in Digital Forensics	PTUK

2. Course resources

Indicative resources for Teaching and Learning			
MODULE TITLE	**Foundations of Digital Forensics**		
INDICATIVE LEARNING RESOURCES - The following list is offered as an indication of the type & level of information that you are expected to consult. Further guidance will be provided by the Module Convener.			
Basic reading: 1. *Computer Forensics and Cyber Crime: An Introduction (3rd Edition)* by Marjie T. Britz, 2013. 2. *The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory* (1st Edition). By Michael Hale Ligh, Andrew Case, Aaron Walters. Web-based and electronic resources: 1. https://www.memoryanalysis.net/amf 2. Computer Forensics World: http://www.computerforensicsworld.com/ 3. Computer Forensic Services: http://www.computer-forensic.com/ 4. Digital Forensic Magazine: http://www.digitalforensicsmagazine.com/			

Indicative resources for Teaching and Learning			
MODULE TITLE:	Digital Forensic Procedures		
INDICATIVE LEARNING RESOURCES - The following list is offered as an indication of the type & level of infomation that you are expected to consult. Further guidance will be provided by the Module Convener.			
Core reading (This material will be used throughout the course, you may indicate the percentage or even the chapter(s) of the book(s) that will be covered):			

The material that will be covered during the semester is:

- Digital Forensic Techniques and Tools
- Digital Forensics Evidence Acquisition
- Internet investigation
- Introduction to Database Forensics
- Database forensic techniques and tools
- Windows Artifacts – closed source operating systems
- Linux Artifacts - open source operating systems
- Memory Analysis

Web-based and electronic resources:

1- EMERALD Database
2- EBSCO Database
3- KNOVEL Database
4- Computer Forensic Training Center Online http://www.cftco.com/
5- Computer Forensics World http://www.computerforensicsworld.com/
6- Computer Security-related organizations : CERT, SANS, CIS, CASPR, CSI, CIAO, DRII, ISSA, IATFF, I2SF, NIAP, CSRC, OWASP

Journals, publications:

1- The International Journal of Digital Forensics & Incident Response

Required Software or Hardware:

1- Hardware:
   - Desktop computers & workstations & server
   - Memory cards
   - Smartphones

- Computer network and connection to internet

2- Software:

- Operating system windows and Linux
- Database SQL and NoSQL e.g. MySQL and MongoDB
- FTK

Template for Indicative resources for Teaching and Learning

MODULE TITLE:	Legal aspects of Digital Forensics

INDICATIVE LEARNING RESOURCES - The following list is offered as an indication of the type & level of information that you are expected to consult. Further guidance will be provided by the Module Convener.

Web based and electronic resources:

1- IEEE Xplore digital library
2- ACM digital library
3- EBSCO database
4- SpringerLink database
5- ProQuest database

Template for Indicative resources for Teaching and Learning

MODULE TITLE:	Business Aspects of Digital Forensics

INDICATIVE LEARNING RESOURCES - The following list is offered as an indication of the type & level of information that you are expected to consult. Further guidance will be provided by the Module Convener.

Basic reading:

1. Business Aspects of Digital Forensics and Ethics (FORC developed textbook)

Web based and electronic resources:

2. NIST Computer Security Resource Centre: https://csrc.nist.gov/publications/sp800

3. IEEE Xplore digital library
4. ACM digital library
5. EBSCO database
6. SpringerLink database
7. ProQuest database

Other resources:

1. Computer Security-related organizations : CERT, SANS, CIS, CASPR, CSI, CIAO, DRII, ISSA, IATFF, I2SF, NIAP, CSRC, OWASP

Template for Indicative resources for Teaching and Learning

MODULE TITLE:	Digital Investigation Tools and Techniques

INDICATIVE LEARNING RESOURCES - The following list is offered as an indication of the type & level of information that you are expected to consult. Further guidance will be provided by the Module Convener.

Basic reading: Digital Investigation Techniques and Tools

Web based and electronic resources:

7- EMERALD Database
8- EBSCO Database
9- KNOVEL Database
10- Others

Other resources:

8. Computer Forensic Training Center Online http://www.cftco.com/
9. Computer Forensics World http://www.computerforensicsworld.com/
10. Computer Security-related organizations : CERT, SANS, CIS, CASPR, CSI, CIAO, DRII, ISSA, IATFF, I2SF, NIAP, CSRC, OWASP

Template for Indicative resources for Teaching and Learning

MODULE TITLE:	Digital Investigation Tools and Techniques

INDICATIVE LEARNING RESOURCES - The following list is offered as an indication of the type & level of information that you are expected to consult. Further guidance will be provided by the Module Convener.

Basic reading: Network Forensics, FORC Book, 2018.

Other resources:

- Davidoff, S., Ham, J. (2012) Network Forensics- Tracking Hackers through Cyberspace. ISBN: 0132564718
- Brunty, J., Helenek, K. (2012). Social Media Investigation for Law Enforcement. ISBN: 1455731358
- Datt, S. (2016) Learning Network Forensics. ISBN: 9781785282126.

Template for Indicative resources for Teaching and Learning

MODULE TITLE:	Mobile Forensics

INDICATIVE LEARNING RESOURCES - The following list is offered as an indication of the type & level of information that you are expected to consult. Further guidance will be provided by the Module Convener.

Core reading:

1. Rank, W., Effing, W. (2010). **Smart Card Handbook**, 4th Ed. Wiley. Chapters: 8, 12, 19.
2. Mayes, K., & Markantonakis, K. (2008). ***Smart Cards, Tokens, Security and Applications***. Springer. Chapters: 1, 4.
3. Limited, C. (2017). ***Mobile Networks Made Easy: A simplified view of mobile networks for professional audience***.

Web-based and electronic resources:

1. History of Mobile Forensics, NIST Document-3182. https://www.nist.gov/document-3182
2. Inventor Dennis C. Hayes - The Great Idea Finder. http://www.ideafinder.com/history/inventors/hayes.htm
3. AT Commands Reference Guide. https://www.sparkfun.com/datasheets/Cellular%20Modules/AT_Commands_Reference_Guide_r0.pdf
4. ITU-T Rec. V.250 (07/2003) Serial Asynchronous Automatic Dialling And Control. https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-V.250-200307-I!!PDF-E&type=items
5. pySim WiKi. https://osmocom.org/projects/pysim/wiki
6. Rooting SIM Cards, Black Hat Slides. https://media.blackhat.com/us-13/us-13-Nohl-Rooting-SIM-cards-Slides.pdf
7. Guidelines on Mobile Device Forensics, NIST Special Publication 800 – 101 Revision 1, Rick Ayers, Sam Brothers, Wayne Jansen, May 2014. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf
8. ACPO Good Practice Guide for Digital Evidence, Version 5, Janet Williams, March 2012. https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf
9. Best Practice Manual for the Forensic Examination of Digital Technology, ENFSI-BPM-FIT-01

(vs.01), the European Network of Forensic Science Institutes (ENFSI), November 2015. http://enfsi.eu/wp-content/uploads/2016/09/1._forensic_examination_of_digital_technology_0.pdf

10. JTAG Explained (finally!): Why "IoT", Software Security Engineers, and Manufacturers Should Care. Senrio's Blog. September 28, 2016. https://blog.senr.io/blog/jtag-explained
11. JTAG Samsung Galaxy S4 (SGH-I337). Forensics Wiki. July 24, 2013. https://forensicswiki.org/wiki/JTAG_Samsung_Galaxy_S4_(SGH-I337)
12. Chip-Off Forensics: How to Extract data from Damaged Mobile Devices. SalvationDATA. April 4, 2018. https://blog.salvationdata.com/2018/04/04/case-study-chip-off-forensics-how-to-extract-data-from-damaged-mobile-devices
13. Mobile Forensics: Apple Enhanced USB Restricted Mode in iOS 12. SalvationDATA. October 22, 2018. https://blog.salvationdata.com/2018/10/22/case-study-mobile-forensics-apple-enhanced-usb-restricted-mode-in-ios-12
14. iOS 12 Enhances USB Restricted Mode. Oleg Afonin, ElcomSoft Blog. September 20, 2018. https://blog.elcomsoft.com/2018/09/ios-12-enhances-usb-restricted-mode
15. Apple File System Basics. https://developer.apple.com/library/archive/documentation/FileManagement/Conceptual/FileSystemProgrammingGuide/FileSystemOverview/FileSystemOverview.html
16. ABPerson Class. https://developer.apple.com/documentation/addressbook/abperson?language=objc
17. Windows Phone 8.10 MMS (for Lumia 530). http://cheeky4n6monkey.blogspot.com/2015/12/windows-phone-810-mms-for-lumia-530.html
18. An Initial Peep at Windows 10 Mobile (Lumia 435). http://cheeky4n6monkey.blogspot.com/2016/04/an-initial-peep-at-windows-10-mobile.html
19. Cellebrite: What You Need to Know About Cell Phone Forensics - North Star Post 20160223. https://let.snowden.in/2016/02/25/cellebrite-what-you-need-to-know-about-cell-phone-forensics-north-star-post-20160223/
20. Snippets on Cellebrite's Samsung Solution and Blackberry Solution. https://blog.cyberwar.nl/2016/03/snippets-on-cellebrites-samsung-solution-and-blackberry-solution-ocrd-from-legal-complaint-against-competitor/
21. Exploiting Qualcomm EDL Programmers.
    a. https://alephsecurity.com/2018/01/22/qualcomm-edl-1
    b. https://alephsecurity.com/2018/01/22/qualcomm-edl-2
    c. https://alephsecurity.com/2018/01/22/qualcomm-edl-3

d. https://alephsecurity.com/2018/01/22/qualcomm-edl-4
e. https://alephsecurity.com/2018/01/22/qualcomm-edl-5

22. Digital cellular telecommunications system (Phase 2+); Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface (3GPP TS 51.011 version 4.15.0 Release 4). https://www.etsi.org/deliver/etsi_ts/151000_151099/151011/04.15.00_60/ts_151011v041500p.pdf
23. Universal Mobile Telecommunications System (UMTS); LTE; Characteristics of the Universal Subscriber Identity Module (USIM) application (3GPP TS 31.102 version 10.14.1 Release 10). https://www.etsi.org/deliver/etsi_ts/131100_131199/131102/10.14.01_60/ts_131102v101401p.pdf
24. ITU-T Recommendation E.118; Overall network operation, telephone service, service operation and human factors; International operation – General provisions concerning administrations; The international telecommunication charge card. www.itu.int/en/ITU-T/inr/forms/Pages/iin.aspx https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-E.118-200605-I!!PDF-E&type=items
25. HUAWEI ME909s Series LTE Module; V100R001; AT Command Interface Specification. http://download-c.huawei.com/download/downloadCenter?downloadId=50263&version=119077
26. ETSI GSM Technical Specification 11.11; Digital cellular telecommunications system (Phase 2+); Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface (GSM 11.11). https://www.etsi.org/deliver/etsi_gts/11/1111/05.01.00_60/gsmts_1111v050100p.pdf
27. GSM Equipment Related Errors. https://www.micromedia-int.com/en/gsm-2/73-gsm/669-cme-error-gsm-equipment-related-errors
28. ITU-T Recommendation E.212; Overall network operation, telephone service, service operation and human factors; International operation – Maritime mobile service and public land mobile service; The international identification plan for public networks and subscriptions. https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-E.212-201609-I!!PDF-E&type=items
29. 3GPP Technical Specification 03.40; 3rd Generation Partnership Project; Technical Specification Group Terminals; Technical realization of the Short Message Service (SMS); (3GPP TS 03.40). https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=141
30. ETSI Technical Specification GSM 03.40; Digital cellular telecommunications system (Phase 2+); Technical realization of the Short Message Service (SMS); Point-to-Point (PP); (GSM 03.40). https://www.etsi.org/deliver/etsi_gts/03/0340/05.03.00_60/gsmts_0340v050300p.pdf
31. ETSI TS 123.038 Technical Specification; Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Alphabets and language-specific information (3GPP TS 23.038). https://www.etsi.org/deliver/etsi_ts/123000_123099/123038/10.00.00_60/ts_123038v100000p.p

df

32. Complete list of APDU responses. https://www.eftlab.co.uk/index.php/site-map/knowledge-base/118-apdu-response-list

Journals, publications:

1. Ibrahim, Nada; Al Naqbi, Nuha; Iqbal, Farkhund; and AlFandi, Omar, "SIM Card Forensics: Digital Evidence" (2016). *Annual ADFSL Conference on Digital Forensics, Security and Law*. 3. https://commons.erau.edu/adfsl/2016/thursday/3
2. Developing Process for Mobile Device Forensics, Version 3, Cynthia A. Murphy, 2013. https://digital-forensics.sans.org/media/mobile-device-forensic-process-v3.pdf
3. Jusas, V.; Birvinskas, D.; Gahramanov, E.; Methods and Tools of Digital Triage in Forensic Context: Survey and Future Directions. Symmetry 2017, 9, 49. https://www.mdpi.com/2073-8994/9/4/49/pdf

Required Software or Hardware:

1. GSM Modem (unlocked).
2. Putty for Windows or Minicom for Linux.
3. Mobile devices (Android, iOS, etc.) or forensic images of mobile devices.
4. Cellebrite UFED or any other forensic tool that can perform mobile devices extraction and analysis.

Template for Indicative resources for Teaching and Learning

MODULE TITLE:	Emerging Trends in Digital Forensics

INDICATIVE LEARNING RESOURCES - The following list is offered as an indication of the type & level of information that you are expected to consult. Further guidance will be provided by the Module Convener.

Core reading (This material will be used throughout the course, you may indicate the percentage or even the chapter(s) of the book(s) that will be covered):

The material that will be covered during the semester is:

- Internet of Things Forensics

- Applying Social Network Logs in Network Forensic Analysis
- Big Data forensics
- Introduction to Cloud Computing forensics
- Cloud Computing Forensic tools and techniques
- Crypto currency forensics
- Digital Forensic Reverse Engineering fundamentals
- Security Analysis of Image, Video, and Audio Forensics

Web-based and electronic resources:

11- EMERALD Database
12- EBSCO Database
13- KNOVEL Database
14- Computer Forensic Training Center Online http://www.cftco.com/
15- Computer Forensics World http://www.computerforensicsworld.com/
16- Computer Security-related organizations : CERT, SANS, CIS, CASPR, CSI, CIAO, DRII, ISSA, IATFF, I2SF, NIAP, CSRC, OWASP

Journals, publications:

2- International Journal of Cyber-Security and Digital Forensics
3- The International Journal of Digital Forensics & Incident Response

Required Software or Hardware:

3- Hardware:
    - Desktop computers & workstations & server
    - Smartphones
    - Computer network and connection to internet

4- Software:

- Operating system windows and Linux
- Database SQL and NoSQL e.g. MySQL and MongoDB
- FTK
- Cloud storage management software or account to cloud storage systems
- CipherTrace for bitcoin forensic

3.Conclusion

These indicative module resources will form the basis for the delivery of the modules described. However one would expect they will need to be updated to remain current in the future.