June 2019

Next Generation of Evidence Collecting: The Need for Digital Forensics in Criminal Justice Education

Scott H. Belshaw
University of North Texas, scott.belshaw@unt.edu

Follow this and additional works at: https://digitalcommons.kennesaw.edu/jcerp

Part of the Computer Law Commons, Criminology and Criminal Justice Commons, Curriculum and Instruction Commons, and the Technology and Innovation Commons

Next Generation of Evidence Collecting: The Need for Digital Forensics in Criminal Justice Education

Abstract

Digital forensics poses significant challenges to law enforcement as the information found in a computer system is often present at most crime scenes in the form of computer data and cell phones. Digital evidence contained on common devices, such as cell phones and laptops, includes information that can be pertinent to the investigation of crimes. Law enforcement is increasingly identifying the need to be able to process their evidence internally warranting the exploration of the need for digital forensics training as part of a broader study of criminal justice for future law enforcement practitioners. This paper uses telephone surveys of police agencies in the North Texas area to explore their capabilities and need for trained digital forensic examiners (n=42). Findings suggest that digital forensic education is needed as most police examiners are trained first as police officers and secondly as digital forensics examiners. Future education challenges and policy implications are discussed.

Keywords

digital forensics education, digital evidence, criminal justice

Next Generation of Evidence Collecting: The Need for Digital Forensics in Criminal Justice Education

Scott Belshaw[a]

Department of Criminal Justice, University of North Texas, Denton, United States

Please address correspondence to: Scott Belshaw, Ph.D.
Department of Criminal Justice
University of North Texas
Denton, TX 76203
scott.belshaw@unt.edu

[a]Scott Belshaw is an Associate Professor in the Criminal Justice Department at the University of North Texas and Director of the UNT Cyber Forensics Lab.

Abstract

Digital forensics poses significant challenges to law enforcement as information relevant to the investigation is often found in computers and cell phones. Digital evidence contained on common devices, such as cell phones and laptops, includes information that can be pertinent to the investigation of crimes. Law enforcement is increasingly identifying the need to be able to process evidence internally, warranting the exploration of the need for digital forensics training as part of a broader study of criminal justice for future law enforcement practitioners. This paper uses telephone surveys of police agencies in the North Texas area to explore their capabilities and need for trained digital forensic examiners (n=42). Findings suggest that digital forensic education is needed as most police examiners are trained first as police officers and secondly as digital forensics examiners. Future education challenges and policy implications are discussed.

Key words: digital forensics education, digital evidence, criminal justice

2

Introduction

Cyber security is an ever-changing field and has become the latest trend in computer science and criminal justice. Recent events such as the hacking from foreign governments and state entities in the US elections as well as revelations by several former members of the intelligence community have brought these issues to the forefront of public attention. The internet is flooded with information on protective measures people can take to defend themselves against illegal intrusions from hackers or foreign governments, however, in criminal justice, most cyber security efforts occur at local and state level jurisdictions in the handling of everyday cases. While prior studies have established an argument for criminal justice programs training students in cyber security to prepare them for changes in the field (Nodeland, Belshaw and Saber, 2018), one endeavor that has received less attention is the use and handling of digital evidence by law enforcement. This article seeks to address the need for criminal justice programs to prepare students, and future law enforcement personnel, in the use and handling of digital evidence just as programs have offered classes in crime scene evidence collection, criminalistics and forensic science.

In the early 1980s, forensic science programs emerged to address the growing need for training law enforcement in the handling of "blood and guts" evidence offering classes in crime scene collection and accident reconstruction as well as blood and serology collection and analysis (Garfinkel, 2011). More specifically, these courses allowed students to understand the fundamentals of investigating homicides, sexual assaults and automobile accidents. As technology has become an integral part of daily life for most Americans, the collection and use of digital evidence has similarly become a common part of many criminal and civil investigations (Garfinkel, 2013). Further, digital evidence is no longer restricted to the

3

prosecution of e-crime, but is used to prosecute all types of crimes, as suspects' e-mail accounts or mobile phone files may contain digital evidence regarding "what a person has been doing, whom they been interacting with, and where they have been" (Carter, 2013: 28). For example, in 2005, a floppy disk provided the critical evidence that led investigators to the BTK serial killer who had taken the lives of at least 10 victims and eluded police capture since 1974 (Digital, 2016). Despite the use of digital forensics in every day case handling, the field of digital forensics has rarely been introduced into "crime fighting" curricula at universities.

The uniqueness and newness of this field is demonstrated in the lack of attention given to the field of digital forensics by the US Bureau of Labor Statistics (BLS). The BLS does provide data for the related occupation of information security analysts, who earn a median salary of $95,510 per year (Information, 2018). The employment outlook for digital forensics examiners and investigators is very favorable due to the rapid growth of digital data in criminal schemes and the need for trained people to investigate them (Information, 2018). BLS has concluded that the number of information security analysts is expected to grow by 28% between 2016 and 2026 (2018).

The electronic trail offenders leave behind requires the investigatory skills of a trained digital forensics analyst for retrieval. Private sector vendors are actively promoting and selling their software and hardware solutions. While these tools facilitate the completion of these analyses among law enforcement, this only increases the need for training law enforcement professionals who are both able to use these programs but also understand the rules of evidence and investigatory processes. To this end, law enforcement agencies are incorporating the collection and analysis of digital evidence, also known as computer forensics, into their

4

infrastructures in an effort to fight cybercrime and to collect relevant digital evidence for all crimes (Digital, 2016).

The Practice and Pedagogy of Digital Forensics

Over the past 20 years, the increasing use of personal computers coupled with the spread of internet access across the globe has accompanied a new wave of criminal activity. Historically, criminal justice practitioners were tasked with recovering and preserving evidence in the physical world, but are now increasingly facing new challenges in completing these same tasks in the digital world (Garfinkel, 2013). Digital information often presents itself inside a device as contraband, evidence, and/or an instrument used to facilitate a crime (Vincze, 2016). The complexity of this issue is demonstrated in the variety of realms of digital forensics including computer forensics, network forensics, mobile device forensics, and memory forensics (Bulbul, 2013; Garfinkel, 2013; Lang et al., 2014; Oparnica, 2016; Tu, 2012). The development and prevalence of cloud-based computing further signifies the complexity of this type of evidence and encompasses yet another area within which digital forensics practitioners must be prepared to recover and preserve evidence (Vincze, 2016). In many ways, digital forensics is the product of the intersection of the practices of law and computer science (Lang et al., 2014), but to take that concept further, the many uses of digital forensics necessitate considerations of interdisciplinary study including business, finance, ethics, accounting, IT and network management (Liu, 2006).

Early attempts at creating a digital forensics curriculum began with a need for a clear and urgent instruction of criminal justice and computer science (Liu, 2006). Specifically, Liu (2006, 2010) identified several challenges in developing this curriculum including:

1) utilizing an instructor with in depth knowledge of several typically unrelated fields,

5

2) incorporating a variety of pre-requisites or testing prior to entrance into the program,

3) substantial start-up costs, and

4) locating an appropriate textbook.

To overcome these challenges, Liu (2006, 2010) identified three models that could be used to design an undergraduate curriculum for digital forensics. The first approach, or the 'for Dummies' approach, meets an immediate need to train a diverse group of people in common situations, but this model will only work well addressing very basic needs. The revamp, or 'patch', approach, utilizes an existing program (e.g. a criminal justice bachelor's program) and inserts digital forensics subject matter creating a new, hybrid program. The last model, or the practitioner's model, incorporates industry needs in developing program subject matter.

Tu and colleagues (2012) further sought the development of a strong digital forensics education program in response to nationwide losses resulting from computer crime. Their objective was to train a suitable workforce prepared to effectively investigate computer crimes. They identified several digital forensics modules that would be beneficial in the fight against cybercrime. First, they established the importance of training and practice using popular forensic tools, such as Encase, FTK, Helix, and WinHex (Tu et al., 2012). They further argued for counter-investigative skills training that might be necessary during encounters with perpetrators well-versed and adept in cybercrime and hacking (Tu et al., 2012).

Alva and Endicott-Popovsky (2012) argue the importance of digital forensics curriculum for law students, and, the same reasoning could be extended to any digital forensic practitioner. They argue the importance of equipping students with knowledge of basic computer literacy, the digital forensics process, knowledge of the Federal Rules of Evidence including how they apply to electronic evidence, and case law pertinent to digital evidence (Alva & Endicott-Popovsky,

6

2012). Similarly, the admission of digital evidence in court is one of the most important considerations in the development of a case utilizing digital forensics. Forensic investigators and prosecutors may feel frustrated and/or see a delay in the processing of a case if digital evidence is deemed inadmissible. Lang and colleagues (2014) argue that training forensics experts in digital forensics as expert witnesses with the ability to testify in court may help to alleviate some of this strain. They further argue for the development of a standardized curriculum for digital forensics experts thereby establishing a minimum skill set that graduates of these programs should possess (Lang et al., 2014). Numerous universities also have digital forensics labs that students can learn from and receive hands on training in the software that is used in conducting forensics examinations. Universities such as Dixie State University in St. George, Utah and the University of North Texas Cyber Forensics Lab offer the latest software training in the digital forensics field.

As previously discussed, the breadth and reach of technology and the internet is continually growing. In 2018, roughly 89% of adults in America reported having access to the internet and 98% of 18-29 year olds are regularly online (Internet, 2018). Coupled with this growth are challenges presented to law enforcement in building and maintaining an educated workforce in digital forensic investigations. For example, Oparnica (2016) argues that there is a lack of well-developed and comprehensive up-to-date educational programs in digital forensics. He offers his insight into the many challenges that face developing such a program based on his personal observations.

> "I took part in fabricating images for mobile telephone forensics training… It took 3 months of around the clock work of 6 college students to create a 'near-real' image of a mobile telephone…With such slow development, all efforts to this end can seem futile…in the one-year time frame you need to develop the course, you can find yourself in trouble: the knowledge you built into the course or some part of it will already be obsolete" (Oparnica, 2016:144).

7

Research Design

In order to gain additional information regarding the need for digital forensics training among law enforcement, we surveyed Texas police agencies on their processing of digital forensic evidence. Specifically, the data for this study were obtained utilizing a convenience sample of Texas police agencies. We contacted fifty-nine Texas police agencies and administered telephone surveys by requesting their participation in response to a series of questions regarding their processing of digital evidence (N=59). We contacted both large and small agencies in order to obtain a more complete picture of the need for digital forensics training among law enforcement agencies in Texas (see appendix A). Forty-two (n=42) of the contacted agencies responded to the following set of questions regarding their digital forensic processing capabilities:

- Question 1: Does your agency have the ability to process digital evidence internally or do you send it to an outside lab?
  - If your agency does have the ability to process digital evidence internally, what types of devices can they process (cell phones, tablets, computers, GPS, skimmers, and/or other devices)?
- Question 2: How many employees are assigned to process digital evidence and are they employed as full-time or part-time examiners? Is their role as an examiner a secondary assignment or is this their primary duty?
- Question 3: Have these employees received training in digital forensics that would qualify them to testify as expert witnesses?

Results

In order to determine the extent to which law enforcement agencies in Texas process their own digital evidence, we asked responding agencies to report whether they process their digital evidence internally or externally through an outside lab. Sixteen of these agencies reported that they process evidence entirely internally, 15 process their digital evidence entirely externally, and 11 process this evidence both internally and externally. In total, 64% of agencies, or 27,

8

reported they process at least some digital evidence internally. These agencies are derived from Small departments consisting of a small agency (1- 25 officers), medium department (26-150 officers) and large department (150 officers and above). Notwithstanding the size of the department, this finding alone suggests the importance digital forensics training for future law enforcement officers as more than half of surveyed departments process digital evidence internally. Responses to the remaining questions are reported only for agencies responding they process at least some of their digital evidence internally[1].

All responding agencies reported the ability to recover and process digital evidence from cell phones. The majority of agencies reported the ability to internally process digital evidence from computers (77%), tablets (73%), external storage devices (69%), DVRs (65%), and skimmers (69%). Finally, some agencies reported the ability to internally process digital evidence from GPS devices (12%), video (>1%), and from drones (>1%). Agencies were further asked whether employees assigned to process this evidence worked as full-time or part-time examiners and whether their role as an examiner was a secondary assignment or their primary duty. The majority of responding agencies, 62%, reported at least 1 part time employee primarily or secondarily tasked with processing digital evidence for the department. The remaining 38% of agencies reported 2 or more at least part-time employees who were primarily tasked with internally processing digital evidence. In sum, most of the surveyed agencies reported a single employee responsible for processing digital evidence with several agencies reporting up to 5 employees.

Next, agencies were asked whether the employee(s) tasked with processing digital evidence had received training in digital forensics that would qualify them to testify as expert

---

[1]One agency that reported they process their digital evidence externally provided responses to additional questions, but was omitted from the discussion as the available data did not allow for a summary of all externally processed agencies.

9

witnesses. Seventy-seven percent of responding agencies who process at least some of their digital evidence internally reported that the employee(s) tasked with processing this evidence had received training qualifying them to testify as expert witnesses. For the most part, this type of qualified training could be just a few days at an online course written by the software company. Very little extensive training is given to these officers. This further suggests the importance of digital forensics training and standardization of digital forensics investigations, as examiners are tasked with processing digital evidence as well as providing expert testimony as to the information that is obtained.

These data provide support for the training of law enforcement in digital forensics as many departments are processing their digital evidence internally. Many of the officers processing this evidence do so as a secondary responsibility, suggesting that any officer could at some point be tasked with this role. Most often, officers working in digital forensics have very little education in computers, much less digital forensic software. It is not uncommon for a police agency to purchase a software package, such as Cellebrite (www.cellebrite.com), and its related training package to ask a currently sworn officer to volunteer time to examine digital data on the side. This is done mainly for budgetary reasons, as training and hiring a full time digital forensics examiner can often be very costly. As such, university training and curricula would provide law enforcement agencies with new officers with a more diverse skill set with some experience and understanding of the processing of digital evidence.

The Future of Digital Forensics Education in Criminal Justice

As discussed, digital forensics investigation requires a diverse skill set, knowledge of a variety of subject matter, and is in demand by law enforcement agencies. The data collected for this study speak to the need for training criminal justice professionals with the ability to process

and explain this evidence. Criminal justice programs are in a prime position to provide digital forensics training and education as many aspiring law enforcement officers already self-select into these programs. To this end, the inclusion of four subject areas have been previously recommended for inclusion into a digital forensics program including computer science and foundations (cryptography and security, communication and network, systems and analysis); procedures, methods, and policies (forensic science/criminology, incident investigation, the U.S. government); legal system and law (legal procedure/ethics, computer/business law, constitutional law); and computer forensics (data seizure and preservation, digital evidence analysis, documentation and presentation) (Liu, 2016). While some of these courses exist in many existing criminal justice programs, the inclusion of additional cross-disciplinary courses in the completion of a criminal justice degree would facilitate digital forensics training among university students. The inclusion of specific courses will provide future criminal justice practitioners with digital investigatory skills in addition to traditional training in both the legal procedures and ethical boundaries for work in law enforcement as well as prepare them with the technical skills to properly carry out digital investigations and secure/handle digital evidence.

At least two universities, University of Alabama at Birmingham and University of Maryland, have successfully implemented digital forensics degree offerings into their criminal justice programs. At the University of Maryland, for example, students have the opportunity to (Digital, n.d.):

- Create an investigation plan for a digital forensics incident
- Conduct a mobile incident response and investigation based on a classroom scenario
- Use appropriate tools and procedures to check for the use of anti-forensics techniques
- Conduct a Linux/Windows/Mac machine image investigation using FTK/EnCase

11

- Identify malicious software, network activity, suspect traffic, and intrusion artifacts through a review and analysis of artifacts
- Conduct a digital forensic investigation in a challenging environment

These tasks are completed as part of a comprehensive Digital Forensics and Cyber Investigation Master's Degree. The program further promotes developing student skills in digital evidence preservation, conducting hands on digital forensic searches, and presenting digital forensics in court as an expert witness (Digital, n.d.). Similarly, University of Alabama at Birmingham's Bachelor of Science in Digital Forensics is situated in the Department of Criminal Justice. This program seeks to:

> "provide graduates with the tools they need in computer programming and operations to work effectively within a computer environment, and also the skills needed to understand the behavior of those who may be a threat to computer systems and/or engage in cybercrime. Additionally, graduates will have an understanding of the legal systems and processes necessary to gather digital evidence and support a computer investigation in court if necessary" (Bachelor, n.d.).

This program indicates that students graduating from the program will be prepared to work in both entry and advanced level positions at all levels of law enforcement as well as the private sector (Bachelor, n.d.). Both of these programs have incorporated the subject areas previously discussed in successfully developing comprehensive digital forensics programs in criminal justice.

Criminal justice programs seeking to develop digital forensics of their own may face several challenges, for example, the ever-changing nature of the field (Oparnica, 2016). Modifying pre-existing courses may be one approach to overcome this hurdle. University faculty regularly update their courses for each new semester, therefore modifying existing courses with up-to-date practices in digital forensics would ensure that faculty are actively involved in current digital forensic practices to provide students with relevant and practical training. Additionally,

12

this curriculum can provide a strong foundational approach to digital forensics by offering courses in the most common operating systems (e.g. NTFS/Windows & Mac) as well as those programs that teach the most popular digital forensic tools (e.g. Encase, Access data-FTK, Cellebrite, Oxygen Forensics etc.) (Alva & Endicott-Popovsky, 2012; Tu et al., 2012; Lang et al., 2014) (see table 1 for a complete listing).

[Insert Table 1 about here]

Another obstacle that may present itself is the interdisciplinary nature of digital forensics. Previous attempts at implementing a digital forensics program struggled to find faculty to teach these courses who were up to date in the subject matter and qualified to teach the courses. For example, among programs surveyed, the difficulty of finding and recruiting high quality faculty to teach on the unique individual aspects within a given module proved challenging (Liu, 2010; Lang et al., 2014; Tu et al., 2012). Professional development among faculty teaching these courses may be one solution to ensure they maintain and develop their knowledge and skill set to best deliver the courses to students. Another short term recommendation may be to recruit adjunct faculty that work in the field to offer a diversification of viewpoints and up to date knowledge of field practice and can enhance the overall knowledge base of a digital forensics program (Lang et al., 2014).

Limitations of this study were clearly focused on the agencies and the type of work and environments they work in. More data is needed to understand the specific training and education level of each officer. This would be for a much bigger study. The focus of this study was to ask the question if more forensic education is needed in this field. Future research could include extensions to the study into larger agencies, as one example, but could also include

13

pedagogical research into ways to create and share sample data sets for student analysis across institutions, leveraging the burden of creating forensic case studies.

The field of digital forensics has changed enormously in a very short period of time. There is an extremely high demand for practitioners in this field. Hands on training and experience in numerous software packages at the colleges can help prepare future police officers and forensic examiners for the processing of digital evidence from the crime scene to the courthouse. According to the literature that has been reviewed and discussed in this paper, the best way to resolve this personnel crisis is to design and implement effective digital forensics curricula at universities around the world. This education could include training in the latest software and forensic techniques that are used and needed in the field. An example of this would be cell phone encryption that changes almost daily. This would help for law enforcement to be on the cutting edge of this technology so they can be ready for the latest update that enters the market. When educating this next generation of criminalists, it is absolutely necessary to focus on a strong foundational approach with an emphasis in continued, lifelong learning in students. Only in this way will academia be able to conceivably and sustainably meet this need. In order to learn from the lessons of the past, it is necessary to consider what has worked and what has failed in the efforts of others. Moving forward, we must be willing to adapt and react quickly to this constantly evolving industry.

14

Appendix A. North Texas Law Enforcement Agencies Contacted to Participate in the Survey

Abilene PD

Allen PD

Amarillo PD

Anna PD

Azle PD

Aubrey PD

Austin PD

Beaumont PD

Bedford PD

Brownwood PD

Canton PD

Cedar Hill PD

College Station PD

Colony PD

Corpus Christi PD

Corsicana PD

Dallas ISD PD

Desoto PD

Euless PD

Fairview PD

Farmers Branch PD

Farmersville PD

Fort Worth PD

Gainesville PD

Garland PD

Grand Prairie PD

Haltom City PD

Houston PD

Howe PD

Hurst PD

Irving PD

Jacksboro PD

Kaufman PD

Keller PD

Krum PD

Lancaster PD

Laredo PD

Longview PD

Lubbock PD

Mesquite PD

Mineral Wells PD

Nacogdoches PD

Odessa PD

Plainview PD

Port Arthur PD

N. Richland Hills PD

Roanoke PD

Rowlett

Plano PD

San Angelo PD

Seguin PD

Sherman PD

Southlake PD

Stephenville PD

Temple PD

Van Alstyne PD

Waxahachie PD

Wichita Falls PD

Wills Point PD

15

References

Alva, A., & Endicott-Popovsky, B. (2012). Digital evidence education in schools of law. *Journal of Digital Forensics, Security and Law*, *7*(2), 5.

Bachelor of Science in Criminal Justice. (n.d.). In *The University of Alabama at Birmingham*.

Retrieved December 8, 2018, from

https://www.uab.edu/cas/criminaljustice/undergraduate/digital-forensics

Bulbul, H. I., Yavuzcan, H. G., & Ozel, M. (2013). Digital forensics: an analytical crime scene procedure model (ACSPM). *Forensic science international*, *233*(1-3), 244-256.

Carter, D. L. (2013). *Homicide process mapping: Best practices for increasing homicide*

clearances. Institute for Intergovernmental Research.

Digital Evidence and Forensics. (2016, April 14). In National Institute of Justice. Retrieved July

9, 2018, from https://www.nij.gov/topics/forensics/evidence/digital/Pages/welcome.aspx

Digital Forensics and Cyber Investigation Master's Degree. (n.d.). In *University of Maryland*

University College. Retrieved December 8, 2018, from https://www.umuc.edu/academic-

programs/masters-degrees/digital-forensics-cyber-investigation-ms.cfm

Garfinkel, S. (2011). Every last byte. *Journal of Digital Forensics, Security and Law,* 6(2):7-8.

Garfinkel, S. L. (2013). Digital Forensics. *American Scientist*, 101(5), 370.

Information Security Analysts. (2018, April 13). In Bureau of Labor Statistics. Retrieved July 9,

2018, from https://www.bls.gov/ooh/computer-and-information-technology/information-

security-analysts.htm

Internet/Broadband Fact Sheet. (2018, February 5). In Pew Research Center Internet &

Technology. Retrieved July 9, 2018, from http://www.pewinternet.org/fact-sheet/internet-

broadband/

Lang, A., Bashir, M., Campbell, R., & DeStefano, L. (2014). Developing a new digital forensics

curriculum. *Digital Investigation*, S76-S84.

16

Liu, J. (2006). Developing an Innovative Baccalaureate Program in Computer Forensics. *Frontiers in Education* (pp. S1H-1 - S1H-6). San Diego, CA: IEEE.

Liu, J. (2010). Implementing a Baccalaureate Program in Computer Forensics. *Consortium for Computing Sciences in Colleges* (pp. 101 - 109). Villanova, PA: CCSC.

Nodeland, B., Belshaw, S., & Saber, M. (2018). Teaching Cybersecurity to Criminal Justice Majors. *Journal of Criminal Justice Education*, 1-20.

Oparnica, G. (2016). Digital Evidence and Digital Forensic Education. *Digital Evidence and Electronic Signature Law Review*, 143-147.

Tu, M., Xu, D., Wira, S., Balan, C., & Cronin, K. (2012). On the Development of a Digital Forensics Curriculum. *Journal of Digital Forensics, Security and Law*, 13-32.

Vincze, E. A. (2016). Challenges in Digital Forensics. *Police Practice and Research*, 183-194.

17

Table 1: Forensic Software

Name of Software	OS Platform	License Type	Description of Software
Autopsy	Windows, macOS, Linux	GPL	A digital forensics platform and GUI to The Sleuth Kit
COFEE	Windows	proprietary	A suite of tools for Windows developed by Microsoft
Digital Forensics Framework	Unix-like/Windows	GPL	Framework and user interfaces dedicated to Digital Forensics
EPRB	Windows	proprietary	Set of tools for encrypted systems & data decryption and password recovery
EnCase	Windows	proprietary	Digital forensics suite created by Guidance Software
FTK-Accessdata	Windows	proprietary	Multi-purpose tool, FTK is a court-cited digital investigations platform built for speed, stability and ease of use.

18

ISEEK[2]	Windows	proprietary	Hybrid-forensics tool running only in memory - designed for large networked environments
Netherlands Forensic Institute / Xiraf[3]	n/a	proprietary	Computer-forensic online service.
Open Computer Forensics Architecture	Linux	LGPL/GPL	Computer forensics framework for CF-Lab environment
OSForensics[4][5]	Windows	proprietary	Multi-purpose forensic tool
PTK Forensics	LAMP	proprietary	GUI for The Sleuth Kit
SafeBack[6]	N/a	proprietary	Digital media (evidence) acquisition and backup
SANS Investigative Forensics Toolkit - SIFT	Ubuntu	proprietary	Multi-purpose forensic operating system
Celebrite	Windows	proprietary	Full range of digital forensic software to provide access to mobile devices, social media, and cloud data sources.

19

Oxygen Forensics	Windows/Mac OS	proprietary	Digital forensic investigation software for government, law enforcement, and enterprise organizations

20