Author: Emily Winfield
Marketing Assistant, North America

APPLICATION NOTE

TECHNOLOGY IN DIGITAL FORENSICS

With the rapid increase in internet and digital media use, cybercrime is at an all-time high. It is reported that about 59% of Americans have experienced cybercrime in some way, and it is predicted that cybercrime will cost the world $10.5 trillion annually by 2025*. That said, protecting personal and professional data online has never been more important. In order for digital forensic teams to resolve these crimes efficiently and to quality standards, it is crucial for them to take advantage of the most modern and intelligent technology.

This article will focus on inspection systems that used to help examine, extract, and document digital evidence which can be used to solve cybercrime cases.

WHAT IS DIGITAL FORENSICS?

Digital forensics is a subfield of forensics that focuses primarily on the recovery and examination of data from digital devices that may be connected to cybercrime activity. The main objective of the process is to gather and analyze data in a way that preserves any evidence in its most authentic form so that it can be utilized in a court case and aid in the conviction of criminals.

Common scenarios in which digital forensics investigations take place are in instances of internet abuse, fraudulent activity, data theft, deliberate or accidental disclosure of company data, or any general cybercriminal activity. Devices that are subject to cybercrime can range anywhere from computers, mobile phones, tablets, hard drives, SD cards, GPS devices, voice recordings, and answering machines.

With cybercrime at an all time high, protecting personal and professional data online has never been more important.

THE NINE PHASES OF DIGITAL FORENSICS

The digital forensics process can be broken down into nine different phases:

1. First Response
   The deployment of a digital forensic team as soon as the crime has been reported.
2. Search and Seizure
   Devices used in the crime are searched for any data and evidence. These devices are seized to prevent further crime.
3. Evidence Collection
   Once the devices are seized, forensic professionals work with law enforcement to identify the goals of the investigation since extracted data may be used as evidence.
4. Securing Evidence
   All data and evidence collected from the device are stores in a secure location for further authentication and accuracy.
5. Data Acquisition
   Forensic specialists retrieve the electronically stored information (ESI) from the device while follow strict procedures to avoid contamination of the data and the device.
6. Data Analysis
   Once the ESI is authenticated, it is analyzed and prepared as data that can be used in court.
7. Evidence Assessment
   After the ESI is identified as evidence, investigators review the evidence in relation to the crime.
8. Documentation and Reporting
   Once the criminal investigation is complete, data and evidence are documented and reported within the guidelines of the court.
9. Expert Witness Testimony
   An expert witness will validate the data for use as evidence and may present it in court.

Of these nine phases, many of them require the use of a microscope that provides extra magnification and other tools that are needed to identify, examine, extract and document evidence properly.

VISION ENGINEERING INSPECTION SYSTEMS

Vision Engineering offers a variety of high performance and ergonomically superior inspection solutions to those working in forensics. With many suitable options to choose from, many digital forensics teams opt for Vision Engineering's unique, patented stereo eyepiece-less and digital microscope systems including, DRV-Z1, Mantis, Lynx EVO, and EVO Cam II.

While each system possesses its own individual set of abilities, they each offer something unique that allows them to be used to simplify each stage of the digital forensics process.

Stereo microscopes with high quality magnification are ideal for the following phases

- Evidence Collection (Phase 3)
- Data Acquisition (Phase 5)
- Data Analysis (Phase 6)
- Evidence Assessment (Phase 7)

During these phases that require analysis and inspection, investigators will search devices for evidence and once found, pass the information onto professionals for furthers inspection and authenticity checks. These checks can be done with the DRV-Z1 where 3D images can be shared among experts based in the same facility or located anywhere in the world. The most common types of evidence collected in a digital forensics case are typically fingerprints, environmental debris, or digital data. While some of these examples are visible to the naked eye, many require additional magnification through a microscope lens. That said, many forensic investigators benefit from an eyepiece-less stereo inspection system, which enables them to identify evidence traces ergonomically and with high quality optics, as well as repair devices such as, PCB boards or small electronics, and extract any potential evidence from them. Vision Engineering systems best suited for these types of requirements include, Mantis, Lynx EVO and DRV-Z1. The technology incorporated in these microscopes allows users to work ergonomically for longer periods of time with no fatigue or strain that is typically associated with traditional microscopes.

Due to the volatility and fragility of the digital evidence, if not handled properly, it can be easily damaged or destroyed. To avoid this, is it important that analysts use equipment that delivers a high quality image during the inspection process.

Digital microscopes with image capture capabilities are ideal for the following phases

- Securing Evidence (Phase 4)
- Documentation and Reporting (Phase 8)

For phases that involve saving confidential information in a secure location, the EVO Cam II and DRV-Z1 have proven to be beneficial for many professionals. EVO Cam II is a digital inspection microscope, and DRV-Z1 a 3D stereo microscope, that allows users to examine their samples under high magnification while also capturing images onto a USB stick. Many forensic experts are drawn to these systems because of their unique features that allows images to be saved privately without the need to place them on a PC or server that could be compromised. It goes without saying that confidentiality and privacy are essential when dealing with forensic evidence, making them both an ideal solution.

	Mantis	Lynx EVO	DRV-Z1	EVO Cam II
Evidence Collection	✓	✓	✓	
Securing Evidence			✓	✓
Data Aquisition	✓	✓	✓	
Data Analysis	✓	✓	✓	
Evidence Assessment	✓	✓	✓	
Documentation and Reporting	✓ *when fitted with a camera PC required*	✓ *when fitted with a camera PC required*	✓	✓

* *Mello, Nick. "Cybercrime to Cost the World $10.5 Trillion Annually by 2025." Institute for Pervasive Cybersecurity, 15 Aug. 2022, https://www.boisestate.edu/cybersecurity/2022/06/16/cybercrime-to-cost-the-world-10-5-trillion-annually-by-2025/.*