There are four phases involved in the handling of digital evidence: identification, collection, acquisition, and preservation.

Identification

Before the collection of digital evidence, our team investigator defined the type of evidence obtained. The digital evidence sought will depend on case type; it can be on devices such as computers, external hard drives, flash drives, routers, and smartphone. Data can be stored on servers in multiple locations; thus retrieving data from these providers is challenging.

Collection

The crime scene was locked by our investigation team when it is reported, suspected, and observed; Our team's first responder found and kept the evidence from contamination and preserved the volatile data on digital devices found at the crime scene. The crime scene was documented, the documentation contains detailed information of collected digital devices, including the device operational state- on, off, standby mode - and its physical characteristics, such as model, serial number, and any markings or other damage.

There is a standard operating procedure (SOP) is followed by our team and is also compulsory to be followed to examine cybercrime that confirms the admissibility of collected proof in a court, also the tools and other resources used to conduct the investigation.

Unique constraints as multiple operating systems and complex network configurations could be encountered, which might require skills and variations in collection procedures. Anti-forensics techniques, such as encryption and steganography, could also be faced during an investigation; thus, Our forensic team investigators were prepared to deal with such constraints. Digital forensics tools such as Forensic Toolkit (FTK) were used to assist in Access Data, Volatile Framework, decrypting files. Our forensic team used a standard forensic toolkit, containing the items needed to document the crime scene, tools for disassembling devices to get evidence, and material for labelling and packing as a Faraday bag for smartphones, wireless signals blocker to and from the digital device.

Collection of volatile data could be encountered. For instance, if a computer encountered is on, volatile evidence (e.g., register, cache, temporary files, connections, and network status) is preserved before the device is power off. If the device is off, then it is collected without turning on. In this case:

Rodger lewis employee of Kericu Company, the device was powered off, so there was no need for the collection of volatile evidence, evidence was collected without powering on the device.

Our team sealed the evidence in tempered proof bags, then labelled and signed by the individual who collected it. Evidence security was maintained throughout the evidence life cycle, from the time it is collected until the trial presentation of court. The measures taken by the investigator during the collection of evidence were documented; Each evidence is labelled, packaged, and carried back to a digital forensics' laboratory.

The chain of custody is vital, and If it is not maintained properly then the evidence may not be admissible in court, It should describe who obtained the evidence and secured it; Where the individual found the evidence and when it was obtained, who had control of the evidence or possession of the evidence as well as where the evidence was stored.

Our team investigators preserved the crime scene and evidence throughout the phase of the case. They maintained a chain of custody, that how they took possession of it. The chain of custody includes the titles, names, and contact information of our team individuals who identified, collected, and acquired the evidence. Our team also recorded the time, date, and the purpose of the transfer in the chain of custody. All of it is documented as well by our team.

Once the items reached the laboratory, the evidence was stored in a tamp proof area, where no one can tamp with the evidence, our laboratory has a procedure, such as a temperature proof seals that indicate that no one has attempted to open or damage the evidence. The evidence was preserved well and protected from extreme temperature, humidity, water damages and other types of damages. Evidence was under supervision all the time, stored in a monitored vault, protected by an alarm system and video surveillance system.

Acquisition

The acquisition can be performed in different ways, varies from the type of digital device. Acquisition procedure for computer hard drive varies from mobile devices, For smartphones if a live acquisition is performed (i.e., static acquisition). Our team preserved the integrity of the evidence during the acquisition of data from evidence. The techniques and tools used were valid and dependable. The limitations were identified and considered before the use of tools and techniques.

The detained digital devices are considered as the main source of case evidence. Data should not be acquired from collected main source devices. Before investigating the file, the team created a copy of digital evidence called as a forensic clone, can also be called as bit by bit copy of the digital evidence, containing files, folders, hard drive partition, operating system, and other data; A cryptographic hash value was attached with every collected file to maintain the integrity. If the copy's contents are a mirror image of the original content that ensure and verify the replicate is an exact copy of the original. A hash value is a mathematical way to map data of an arbitrary size onto data of fixed size using hash codes and digest, few common examples of hash values are SHA-1, SHA-2, and MD5.

Write blocker was used during the copying process to prevent the alteration of data and to prevent the modification of data during the copying process. A different procedure was followed to acquire data from mobile phones and similar devices where memory storage could not be physically removed create an image.

Our team had to perform both Physical and logical extraction for the acquisition process. Physical extraction includes the search for and acquisition of evidence from the place of evidence within a digital device, such as the hard disk or USB. Keyword searches, file carving, and examining unallocated space and partition could be used to conduct a physical search. Logical extraction includes the search for and acquisition of evidence from the file system of a computer operating system, which keeps track of the names and locations of files that are saved on a hard drive or such storage medium. Logical extraction type depends on the digital device, applications on the device, file system, and operating system. Data from active and deleted files, unallocated and unused space, file systems, and encrypted, compressed, and password-protected data can be recovered from logical extraction.
The entire acquisition process was documented as well, containing detailed information about the digital devices from the evidence was extracted, the software and hardware operated to acquire the evidence, when, where, how, why and what evidence was obtained, also the reason it was obtained.

Preservation

Evidence was protected from any modification in preservation. Our team has protected the digital evidence from tampering and maintained the integrity in each phase of the digital evidence handling. From Investigators, crime scene technicians, responders, and digital forensics experts all validate they maintained the integrity during the forensic investigation processes: identification,

collection, acquisition, and other phases; Capability of doing that depends on the digital device and circumstances faced as preserving the data. Our team made sure that evidence was authentic, accurate, complete, convincing, and admissible.

References:

https://www.unodc.org/e4j/en/cybercrime/module-6/key-issues/handling-of-digital-evidence.html