Case 3

Case report generated by:

CSI ID: 5

Name: Sapna

Email ID: sapna@gmail.com

Phone Number: 9876543102

Date: 2024-04-23

Time: 12:53:10

Timezone: IST

1.jpg

1_annotated.jpg

1_annotated_counts.txt

tv: 0

laptop: 1

mouse: 0

remote: 0

keyboard: 0

cell phone: 2

microwave: 0

oven: 0

toaster: 0

Case 3-1-2024-04-23_12-51-57.txt

Date and Time: 2024-04-23 12:51:57

Case Number: Case 3

Evidence Number: 1

Unique Description: SD Card

Notes: dqtwfyguvheij

Device Information:

Device/Media Name: Built In SDXC Reader

Protocol: Secure Digital

Disk Size: 4.1 GB (4075290624 Bytes) (exactly 7959552 512-Byte-Units)

Device Block Size: 512 Bytes

Case 3-2-2024-04-23_12-52-45.txt

Date and Time: 2024-04-23 12:52:45

Case Number: Case 3

Evidence Number: 2

Unique Description: vbew

Notes: enlke

Device Information:

Device/Media Name: Cruzer Blade

Protocol: USB

Disk Size: 30.8 GB (30765219840 Bytes) (exactly 60088320 512-Byte-Units)

Device Block Size: 512 Bytes

ProductID: 0x5567

VendorID: 0x0781 (SanDisk Corporation)

Manufacturer: SanDisk

Free Space: 2.74 GB (2,74,11,08,736 bytes)

Volume UUID: 600F8D97-3EA6-3446-9E48-17E3DD10F639

description_file.txt

laptop: Initial Documentation and Evidence Log: Create a detailed evidence log documenting all actions and transfers. Initial Documentation and Evidence Log: Securely store the evidence log and maintain a clear chain of custody. Short-Term Memory (RAM) Analysis: Extract data from RAM promptly to capture recent computer activities. Short-Term Memory (RAM) Analysis: Use tools like Volatility or Redline for RAM analysis. Short-Term Memory (RAM) Analysis: Document all RAM extraction actions and maintain the chain of custody. Long-Term Storage Device Preservation: Create exact copies of the data on write-once optical media. Long-Term Storage Device Preservation: Seal the original storage medium and transfer it to a responsible party. Long-Term Storage Device Preservation: Maintain locked containers with verified copies for distribution. Live Forensic Process: Document all actions during live system analysis. Live Forensic Process: Use tools like FTK Imager or Helix3 for live system analysis. Live Forensic Process: Establish a trusted network repository and document all transfers. Live Forensic Process: Maintain the chain of custody for any extracted or transferred data. Disk Imaging: Use specialized tools like EnCase or X-Ways Forensics for forensic-grade disk imaging. Disk Imaging: Ensure correct recognition of physical parameters. Disk Imaging: Perform cryptographic verification before and after imaging. Disk Imaging: Document all imaging steps and maintain the chain of custody.

mouse: Data Acquisition: Establish Chain of Custody. Data Acquisition: Identify the Mouse Interface (e.g., USB, Bluetooth). Data Acquisition: Choose Acquisition Method (e.g., USB data extraction, Bluetooth packet capture). Data Acquisition: Acquire Data using write-blocking techniques if applicable. Digital Traces Analysis: Maintain Chain of Custody. Digital Traces Analysis: Utilize Forensic Tools (e.g., Volatility, USBDeview). Digital Traces Analysis: Retrieve Relevant Traces (e.g., mouse movement patterns, clicks, device identification). Device Analysis: Document Examination. Device Analysis: Analyze Device Metadata (e.g., manufacturer, model, serial number). Device Analysis: Review Connection History and Timestamps. Device Analysis: Identify Interaction Patterns (e.g., usage frequency, timestamps of usage).

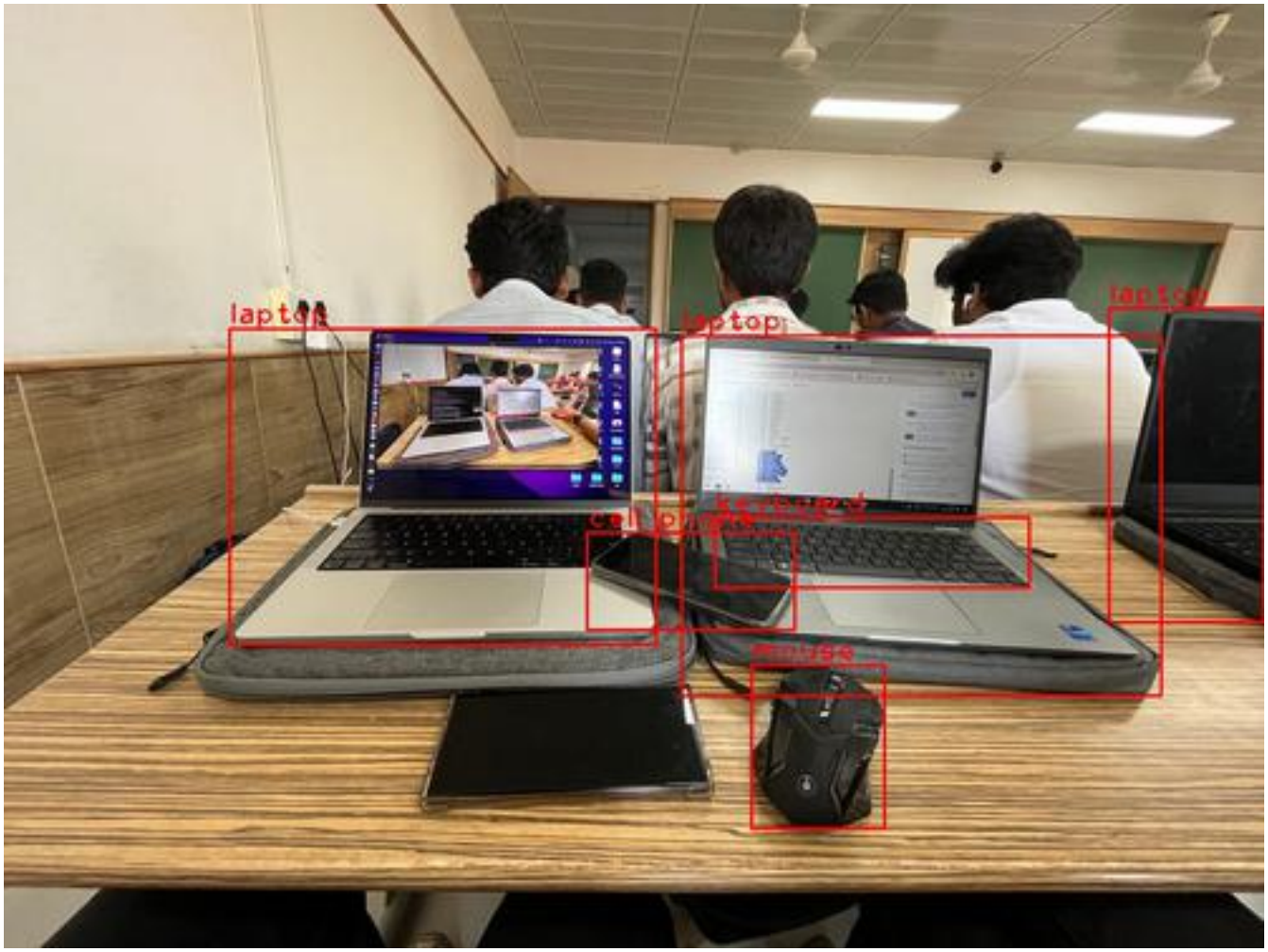
keyboard: Data Acquisition: Establish Chain of Custody. Data Acquisition: Identify the Keyboard Interface (e.g., USB for wired, Bluetooth for wireless). Data Acquisition: Choose Acquisition Method (e.g., USB data extraction, Bluetooth packet capture). Data Acquisition: Acquire Data using write-blocking techniques if applicable. Digital Traces Analysis: Maintain Chain of Custody. Digital Traces Analysis: Utilize Forensic Tools (e.g., Volatility, USBDeview). Digital Traces Analysis: Retrieve Relevant Traces (e.g., keystrokes, keylogging data, device identification). Device Analysis: Document Examination. Device Analysis: Analyze Device Metadata (e.g., manufacturer, model, serial number). Device Analysis: Review Connection History and Timestamps. Device Analysis: Identify Interaction Patterns (e.g., frequency of key presses, timestamps of usage).

cell phone: Cellphone Identification: Establish the purpose and scope of identification to locate relevant digital evidence. Cellphone Identification: Recognize that data may extend beyond the device to cloud accounts or other devices. Cellphone Identification: Document comprehensively to avoid errors that could compromise evidence. Mobile Phone Collection: Gather physical devices including smartphones and other relevant mobile devices. Mobile Phone Collection: Protect digital evidence from contamination by isolating devices from users until forensic acquisition. Mobile Phone Collection: Take measures to isolate devices from data transmission networks to prevent data alteration. Mobile Phone Acquisition: Perform logical extraction using tools like Cellebrite UFED or Oxygen Forensic Detective to collect active data. Mobile Phone Acquisition: Conduct file system extraction with tools such as XRY or Magnet AXIOM to access internal memory and retrieve system files, logs, and database files. Mobile Phone Acquisition: Execute physical extraction using tools like Cellebrite UFED Physical Analyzer or MSAB XAMN to capture the entire contents of the device, including deleted data and unallocated space. Mobile Phone Acquisition: Analyze backup files created when connecting the phone to a

computer using software like iTunes or Oxygen Forensic Detective. Mobile Phone Acquisition: Utilize tools such as Cellebrite UFED Cloud Analyzer or Oxygen Forensic Cloud Extractor to access and acquire data stored in the cloud. Cellphone Data Preservation: Maintain a chain of custody using digital evidence management systems like ADF Digital Evidence Investigator or BlackBag BlackLight to protect digital evidence from modification or tampering. Cellphone Data Preservation: Apply mathematical hashing algorithms with tools like HashCalc or md5deep to create unique hash values, ensuring the integrity of extracted data. Reporting on Mobile Devices: Prepare reports detailing the data extracted from the mobile device using forensic report generation tools such as XRY or Cellebrite Physical Analyzer, formatted for accessibility and review. Reporting on Mobile Devices: Create more in-depth reports when necessary to explain timelines, data types, or specific forensic artifacts using tools like Oxygen Forensic Detective or Magnet AXIOM. Cellphone Forensics Expert Testimony: Select experts with appropriate technical expertise and communication skills. Cellphone Forensics Expert Testimony: Ensure experts can effectively explain technical concepts and forensic procedures in plain language to judges and juries.

pls_work.jpeg

pls_work_annotated.jpg



pls_work_annotated_counts.txt

tv: 0

laptop: 3

mouse: 1

remote: 0

keyboard: 1

cell phone: 1

microwave: 0

oven: 0

toaster: 0