1. In 3-5 sentences, describe what you believe to be an ideal working environment for the digital forensics investigator. Why did you choose the attributes of the working environment that you choose. Identify 3 professional journals that either confirm or dispute your thoughts on the working environment. Did these journals provide insight into the working environment?

Answer:

The Ideal working environment for me as a Digital Forensics Investigator is having a whole room for myself with minimum size of 2x2m and more the better. I would like to have my technical stuff set to one side of room and to the other side lab equipment and storage area to the another side of the room with a long rectangle table at the centre of the room for me to work and black board to the remaining side. The room should be well ventilated and continuous air flow inside the room.

With the above setup I can work without any disturbance and will be able to give my 100%. But the ideal setup I mentioned is not possible in real world scenario especially in case of Digital Forensics Investigator. Which requires not 1 or 2 but involves multiple branches just under Digital Forensics the list increases, if we consider Physical Forensics Investigation as well. The prominent branches in Digital Forensics Namely:

* 1. Computer Forensics
  2. Mobile device forensics
  3. Network forensics
  4. Database forensics

The Knowledge, techniques and equipment vary drastically for each branch and it becomes more complicated when importance and volatility of the evidence comes into picture. The information required for doing the forensic analysis isn’t available at hand every time and the investigator needs to go to crime scene to collect or retrieve them and bring back to lab without causing any damage to it. So, through analysis can be done in the lab.

The article by Rebecca Munday, she mentioned that work of forensic investigator varies depending on the level of experience one has in the field. The Senior level people will involve less hands-on analysis work, instead focusing on talking to law enforcement and other clients to figure out what needs to be investigated, then delegating the work to a team of digital forensics professionals. While the juniors will be doing more hands-on analysis and field work that may put them in working long hours, including weekends.

Reference:

<https://www.unodc.org/e4j/en/cybercrime/module-4/key-issues/standards-and-best-practices-for-digital-forensics.html>

<https://www.bluevoyant.com/knowledge-center/understanding-digital-forensics-process-techniques-and-tools>

<https://www.ignet.gov/sites/default/files/files/Quality_Standards_for_Digital_Forensics_2019.pdf>

<https://www.computerscience.org/careers/computer-forensics-investigator/day-in-the-life/>

<https://www.frontiersin.org/articles/10.3389/fpsyg.2023.1142106/full>

1. What tools do you believe are critical for a forensics investigator to be effective? Why did you choose these tools? what are system requirements for these tools? can you simply put them on any old device? if so, would you? If not, why not? Explain.

Answer:

a. **Computer Forensic Reference Data Sets (CFReDS)**, having proper data to compare and refer play an important in any field. The data can be anything like DNA samples, Blood group, Fingerprints, Facial data and many more which can be used depending on the need of the investigator.

b. **Volatility** : It is a command-line memory analysis for extracting artefacts from memory dumps. It is an open-source, written in python and can be run on Windows, Mac and Linux.

c. **ProDiscover**: It is launched in 2001 to help public and private organizations solve digital crimes. As of 2021, the India-based provider works in over 70 countries with more than 400 clients, including the NIST, NASA, and Wells Fargo. ProDiscover Forensics captures evidence from computer systems for use in forensic investigation to collect, preserve, filter, and analyze evidence. It can run on Windows, Mac and Linux. It has three different versions available depending on the requirement of the investigator and the license need to be purchased.

We cannot put them in any old device has the field of technology is developing rapidly and we will have issue with compatibility of the hardware. As we cannot have different piece of hardware for each of software to run it. We will have issue of security with using old devices which will result in devices getting hacked which results in comprising the analysis.

Reference:

Brendan O’Shaughnessy, “Cyber Sleuths,” University of Notre Dame Stories, accessed January 30, 2020, <https://www.nd.edu/stories/cyber-sleuths/>.

<https://cfreds.nist.gov/>

1. Identify 2 types of data blockers, can these be bought or built? if bought, from where, if built, describe the process to build one of the two types of data blockers.

Answer:

* 1. **USB Condom:** It is a small device that blocks the data transfer when connected to any usb port, allowing only power to pass through.

It can be bought online from any retailers like Amazon, ebay etc..,

Below is the link for the one of that kind of device.

<https://www.amazon.com/FireWire-Condom-Smart-Phone-Protection/dp/B07VX6YHJG/ref=sr_1_2?crid=3TI2930Q6PI55&keywords=usb+condom&qid=1693282220&sprefix=usb+condom%2Caps%2C128&sr=8-2>

* 1. **Camera and Microphone Data Blocker:** It is used to block camera and microphone of the device to prevent unauthorized access to these components. Now-a-days, In Android, we have a built in option to block them on software level.

Or we can buy third party software like Oversight or Micro Snitch for mac OS.

* 1. **Bluetooth data blocker:** It is used to prevent unauthorized pairing or data exchange between devices via Bluetooth connections.

**Reference:**

[**https://www.geckoandfly.com/26071/block-windows-mac-camera-spy/**](https://www.geckoandfly.com/26071/block-windows-mac-camera-spy/)