# Lab 01 – Your Workstation

As an IT professional within an accounting firm, you have been tasked with starting a forensic capability. The business has 150 employees and supports 10 forensic investigations of systems annually (which they are currently outsourcing). They intend to higher one new full time employee to work on investigations. Using available resources, determine the best forensic workstation to use. You can use your background in computer hardware to hand pick relevant items and build a custom system (including extra storage and write protected drive interfaces) or you can seek out options that are pre-built using either the notes in the PowerPoint or other online resources.

You can assume you might have to assess more than one system at a time over a 12-month period, so you will want enough storage for your OS, tools, extracted artifacts, and any images captured (unless you prefer to operate on clones). Your organization has a uniform deployment of 120 desktops with 8GB RAM and 128GB HDD and 50 laptops with 8GB RAM and 256GB SSDs. All disks use a SATA interface.

In less than a page answer the following:

* Would you develop your own system or buy a pre-built one? Why?

I would prefer to buy a pre-built forensic workstation from a vendor. Vendor systems would reduce the time we spend configuring hardware, as well as allow us to purchase and deploy duplicate hardware setups with little difficulty in the future prospect of department expansion. Vendors would also be able to facilitate deals for appropriately timed upgrade cycles.

* What are the specifications of the system you are going with? Why?

There’s a lot of data to keep track of across all the endpoints, so I would address storage last and stock it with as much storage space as I can using the remaining budget. 2 tb storage minimum is a greedy comfort goal. A raid setup would provide local redundancy, and would be an excellent supplement to remote backup services. And a lot of ram (64G minimum) so they can comfortably run several vms at the same time alongside their tools and business software without bogging things down.

* Other than a forensic suite, what additional software do you need and why?

Virtualization software, Remote Backup Services, Accounting software (assumed due to nature of the business), common software loadouts like Microsoft Office.

* What is your total estimated cost of this acquisition (again, excluding the forensic suite)?

$16,000 upper max. realistically expect to use ~$12,000 for core system, and the rest allocated to miscellany and extra beef.

## Scoring

The score will be assessed out of 20 points, 5 points for each prompt. A rubric will be provided in D2L.