I was recruited to start a computer crime unit and started on 11/28/1994. The Regional Electronics and Computer Investigation Section opened on 1/2/1995. 30 years, 5 months, 2 weeks, 5 days (if it's Wednesday 5/21/25).

While the Internet existed – and the world wide web became available on 4/30/1993 (thank you Dr. Tim Berners Lee – not Mr. Gore), it took a while to be accepted and it really didn't "work" until 1995 or 1996, and didn't take off until broadband access became available in the late 90's or early 2000's.

Train, stay current, and train some more. Develop training and provide it. Do your best to find vendor neutral training, FLETC, NCFI, NW3C, something along those lines. Vendor based is fine – but its vendor based, and so narrow in scope. The same goes for certifications – DFCP – NW3C – IACIS are all vendor neutral.

All in wonder tools are necessary today – volumes of data require automated processing. You should still know how to unerase a file, build a boot record, and read a FAT / MFT / whatever manually, be able to partition a hard disk, so you can explain how the tools do what they do.

What happens from "power on to prompt" (the POST and boot process). Making a "neutered boot disk" story, and the native disk compression tools.

Be able to create. Make your own bootable media – learn how. Not because it's "required" but because you will learn about how computers work – and boot – and what an OS does – and that will make you a much better forensic person.

Write a batch file to automate a process – and be able to comment on each line.
What does the file do.bat – do?

```
@ECHO OFF
CD %1
ren *.* %1ack*.*
cd..
echo done
```

Learn from the past and from others. The Steve Jackson Games case story – and the Cincinnati Computer Connection.

Keep notes in real time – and hold onto them. “Why Common Pleas Authority” is required story – The Ohio Search Warrant Manual by Albert Mestemaker (1996-2006) story.

Know how to manually set an IRQ and DMA channel – and know what they are and why your computer needs them. Learn how to terminate a SCSI chain too, you may need to someday. Maybe even write a .PIF file even if Windows doesn’t use them any more or at least configure your Windows explorer to open the tree to C:\. In the 90’s serial ports became “out dated” because they were too slow. Today we use USB all the time – right back to the serial interface because it’s faster. Go figure.

Never resist the urge to validate your tools or challenge the accepted “status quo” – the ACES story (Automated Computer Examination System). It would have worked on Win 95/98 and maybe 2000 and ME (Maybe) – but not on Windows NT that it was built to run on. An example of the designer not knowing how computers work. HTCIA conference story.

Baseline your systems so you can document that they are working properly. Maintain that documentation. Be able to take that to Court with you – and all of the sudden you are a capable, dedicated, and through forensic analyst.

Portable devices have really watered down the quest for the “Holy Grail” – an unaltered and unchanged image of the suspect device or media. Not necessarily a bad thing – just a real thing. Be able to articulate what happened – and why you let it happen. TrueCrypt example.

Maintain a hardware and software archive. Portable device analysis and reporting tools improve in each version. It’s not that they are obtaining more data – they are just improving on their processing, parsing, and display of the data that they have. They “look like” they are finding more because they make locating the data or seeing the data better. In the year between when you process a device and the case goes to court or the defense reviews the evidence the tools will improve. The defense may (I’m not saying they will – but they could) spin that as “smoke and mirrors” – our guy found more stuff than you did. Therefore 1) you suck at your job, or 2) you are too lazy to do the job correctly, or 3) you are purposely concealing data that could be exculpatory or 4) fill in the blank. You either need to be able to locate and run the old version – or explain how the new version “found more stuff” just by demonstrating the difference in the display of the data or GUI changes to the program.

Never hesitate to ask. Email list serves have “fallen by the wayside” – and they never should have. Goback FLETC fix story followed by the Compaq gold paint FLETC story.

First forensic system specs: 01/02/1995

- 80486DX2 @ 66Mhz
- 1 Megabyte of RAM (640K who will ever need more?)
- 2 – 500 MB IDE hard disks
- 5.25” and 3.5” floppy disk drives
- CD-ROM drive
- 9600 baud external modem
- DOS v6.22
- Windows for Workgroups v 3.11
- Norton Desktop for Windows
- Norton Utilities
- Safeback from Sydex
- CPR Utilities
- QEMM (because emm386.sys sucked)
- External SCSI port on an Adaptec card

Current forensic system specs: 05/16/2025

- Talino
- Intel i9 @14900 Ghz
- 128 Gigabytes RAM
- 6 – 4 TB IDE hard disk in RAID
- NAS for 40 TB of archive storage
- Integrated physical write blocked drive access – IDE / SATA / USB 3.x / Firewire / eSATA
- Windows 11
- Tons of tools

The old hands that are around you will be happy to share so that you don’t have to re-invent the wheel. You guys will be required to continue that legacy.