

Lesson 14 — IT Roles & Open Source

Who does what; the open-source ecosystem; how to enter; which course to take next.

IT Landscape

Module 5

Course Finale

Roles are clouds, not boxes

"In real teams, titles overlap. A 'Full-stack Engineer' at a 5-person startup does what a 'Frontend Engineer' + 'Backend Engineer' + 'DevOps Engineer' + 'QA Engineer' do at a 500-person company."

- Same person, **different title** depending on company size and culture.
 - Hold the titles loosely — *use them to know what to search for*, not to box yourself in.
-

The engineering job-family map

Build the product

- **Frontend**
- **Backend**
- **Full-stack**
- **Mobile** (iOS / Android)
- **Embedded** (firmware)
- **Game** (Unity, Unreal)

Keep it running

- **DevOps Engineer**
- **Site Reliability Engineer (SRE)**
- **Platform Engineer**
- **Cloud Engineer**
- **Security Engineer**

As of 2026 — titles drift; the work is what matters.

The data and AI job-family map (as of 2026)

- **Data Engineer** — pipes data around (Airflow, dbt, Spark, Kafka).
- **Data Analyst** — asks questions of data (SQL, dashboards).
- **Data Scientist** — builds statistical / ML models in notebooks.
- **ML Engineer** — puts models into production.
- **AI Engineer** — *new* — builds with LLMs, RAG, and agents.
- **Research Scientist** — academia-adjacent.

The boundaries between these five shifted noticeably in 2024–2026 as LLMs landed. Refresh annually.

The “around engineering” roles

- **Product Manager** — what to build, for whom, why.
- **Designer** — UX, UI, research.
- **Engineering Manager** — people + delivery.
- **Tech Lead** — people-light, technical-direction-heavy.
- **Solutions / Sales Engineer** — technical, customer-facing.
- **Developer Advocate** — community-and-content-facing.
- **Technical Writer · QA / Test Engineer.**

Many people land in IT through these doors without ever writing production code.

Security as its own world

- **Defensive** (Blue Team) — SOC analyst, threat hunter, incident responder.
- **Offensive** (Red Team) — penetration tester, security researcher.
- **Governance, Risk & Compliance (GRC)** — risk, compliance, audit.
- **AppSec / Cloud Security / OT Security** — specializations.

Increasingly its **own career ladder**, not a stop on the engineering one.

*See sibling courses on this platform: **CTF Blue Team** and **CTF Red Team**.*

Open source — what it actually is

"Code anyone can read, anyone can copy, anyone can change. Usually for free."

- Most of the software you use is **built on it**.
 - Every cloud, every browser, every database you've met in this course sits on a tower of open-source pieces.
-

Why open source exists (and why it works)

- **Dogfooding** — maintainers volunteer because they need the tool too.
- **Corporate backing** — many are paid by their employers to work on tools their employers use: *Linux, Kubernetes, Postgres, Python, the LLVM compiler* — all overwhelmingly maintained by paid engineers at large companies.
- **Foundations** — Linux Foundation, Apache, CNCF, Python Software Foundation, Mozilla.

Money + identity + meritocracy + accumulated trust.

Open-source licenses (the 30-second version)

- **MIT / Apache** — very permissive; use however you want, even closed-source.
- **GPL** — you must share changes back if you redistribute.
- **AGPL** — same, even if you only use it as a network service.
- **BSL / SSPL** — newer “source-available”; *not strictly open source*; vendor protection.

~95% of new projects in 2026 use MIT or Apache.

How to “enter” IT without a CS degree

1. Pick **one role** from slides 3–6 that looks interesting.
2. Read its **job-ad language** until it stops feeling foreign.
3. Ship **something tiny in public** — a GitHub project, a blog, a tool, a Substack.
4. Contribute a **one-line fix** to a small open-source project.

The “ship in public” step matters more than any certification.

Which course on *this* platform next?

If you liked...

- Module 2 / building things
- Module 2 + building tools FOR AI
- Module 4 / agents specifically
- Module 3 / security, defending
- Module 3 / security, attacking
- Module 1 / networking, infrastructure
- Module 1 / cloud and ops
- AI ops & safety
- Password cracking / hashing

...take next:

- **Claude & LLMs** (33 lessons)
 - **MCP Servers**
 - **Building Your Own Agents**
 - **CTF Blue Team**
 - **CTF Red Team**
 - **Linux Networking**
 - **Helm Charts** (20 lessons)
 - **AI OpSec + AI Prompt Security**
 - **Hashcat** (10 lessons)
-

The course, in three bullets

- You now have a **map of IT** (*L01*) — frontend / backend / data / infra / security all on one page in your head.
 - You've seen what the **tools actually look like** (*L05*) — IDEs, GitHub, AI assistants — and know the words on a job description aren't magic.
 - You've watched **AI become a real seat at the table** (*L11*) — and you know which sibling course to take to actually build with it.
-

The end — and the start.

"This was a survey course. The map is in your head now. The next step is to go deep on one square of it. Pick a course from slide 11. Or go talk to someone who works in IT — you can keep up now."

Course complete. Continue with the recommended sibling course of your choice — all live in this same repo.

