How to get published in 2600

(or anywhere else)

Two parts of the workshop:

- Part one: getting to the first draft
- Part two: getting from the first draft to a published piece

Part one: getting to the first draft

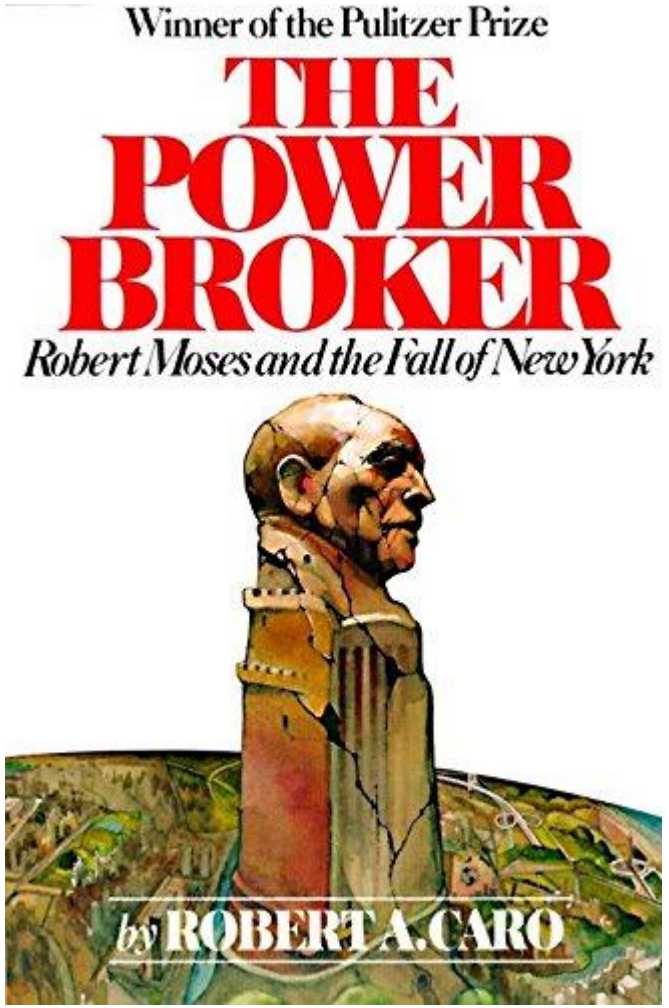
- How to get an idea:
  - read the news
  - look at different tech themes
  - think about issues you have encountered

Part one: getting to the first draft

- Turn idea into outline:
  - two approaches:
    - rant/ramble
    - list of statements or questions

Part one: getting to the first draft

- Turn idea into outline:
  - two approaches:
    - rant/ramble
    - list of statements or questions
  - look through the rant or statements, and find a thesis
    - robert caro's method with outline



Part one: getting to the first draft

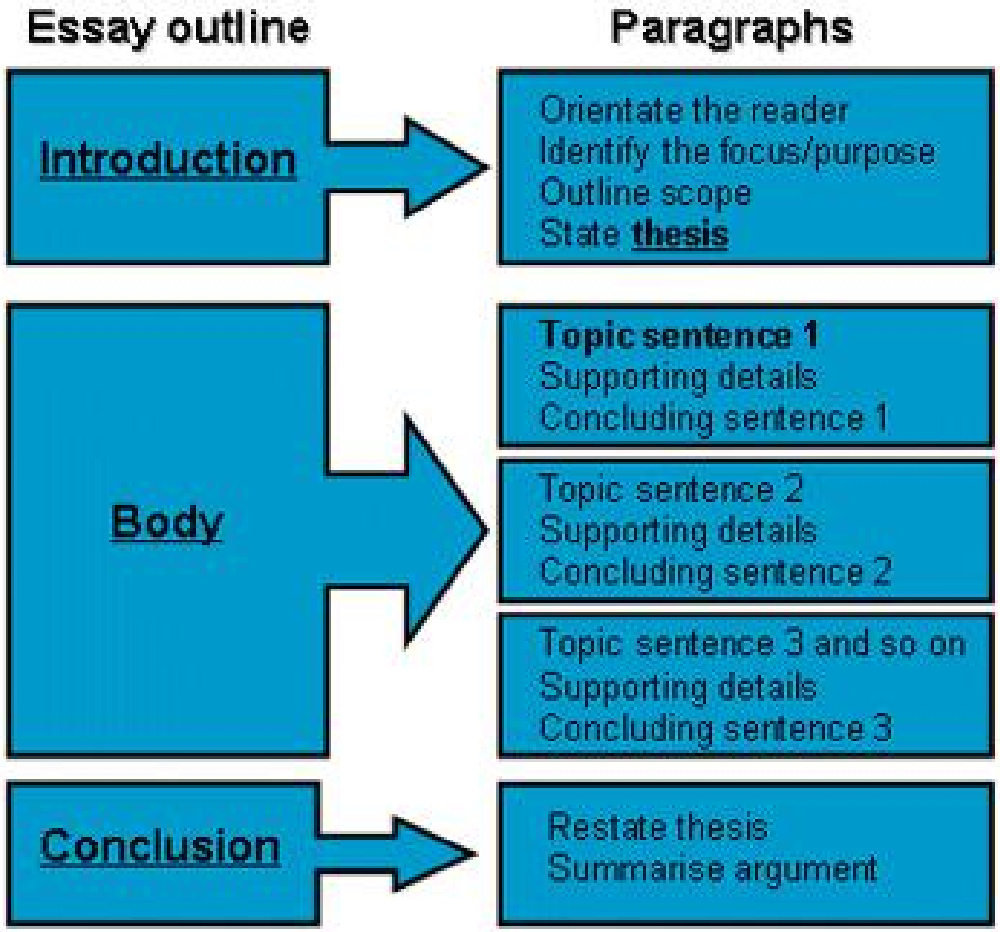
- Turn idea into outline:
  - once you have a thesis, answer the questions:
    - who is my target audience?
    - why do I have something to say?
    - why am I qualified to speak about it?
    - has anyone else addressed the theme?
    - what format do I need? is this for a newspaper? an essay for a book?

Part two: getting from the first draft to published

- General format of an esssay
- Rhetorical devices
- Flow
- Hooks and punches

Part two: getting from the first draft to published

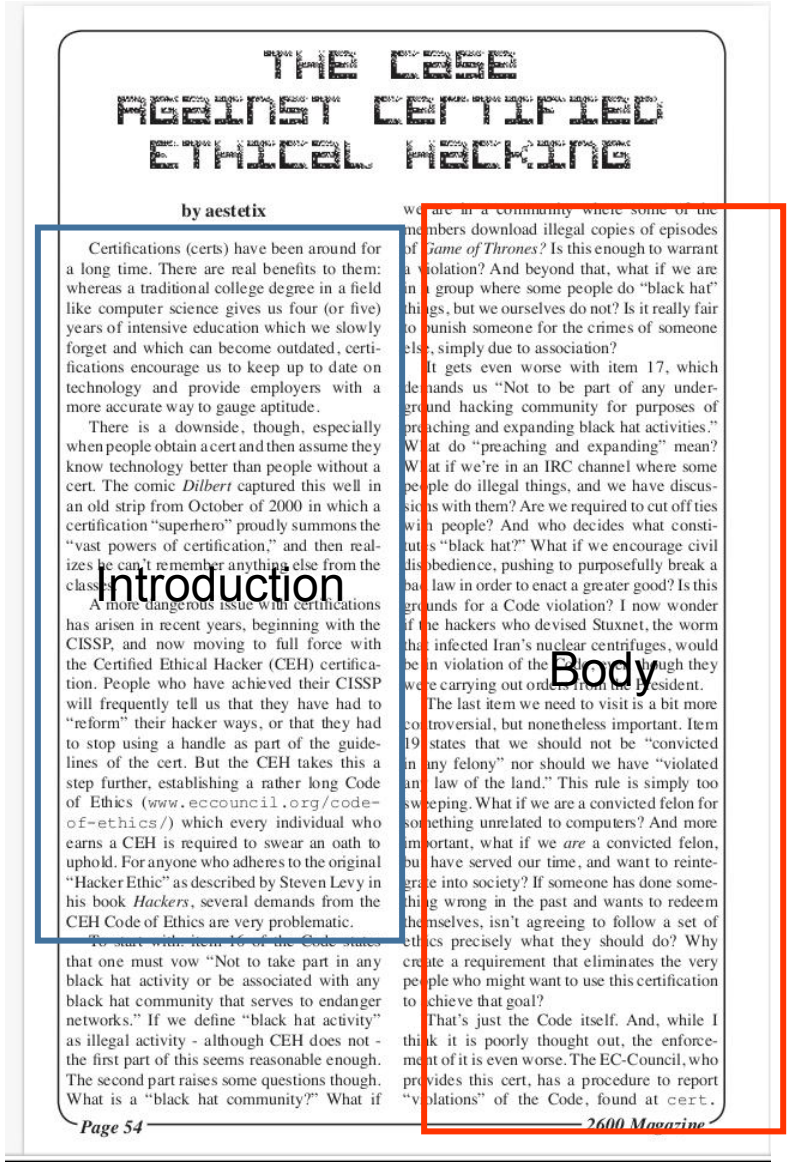
- General format of an esssay



https://i.pinimg.com/originals/fd/00/3c/fd003c4dde6122d3195e7754d336f1f7.gif

Part two: getting from the first draft to published

- General format of an esssay



THE CASE AGAINST CERTIFIED ETHICAL HACKING

by aestetix

Certifications (certs) have been around for a long time. There are real benefits to them: whereas a traditional college degree in a field like computer science gives us four (or five) years of intensive education which we slowly forget and which can become outdated, certifications encourage us to keep up to date on technology and provide employers with a more accurate way to gauge aptitude.

There is a downside, though, especially when people obtain a cert and then assume they know technology better than people without a cert. The comic *Dilbert* captured this well in an old strip from October of 2000 in which a certification "superhero" proudly summons the "vast powers of certification," and then realizes he can't remember anything else from the class.

A more dangerous issue with certifications has arisen in recent years, beginning with the CISSP, and now moving to full force with the Certified Ethical Hacker (CEH) certification. People who have achieved their CISSP will frequently tell us that they have had to "reform" their hacker ways, or that they had to stop using a handle as part of the guidelines of the cert. But the CEH takes this a step further, establishing a rather long Code of Ethics (www.eccouncil.org/code-of-ethics/) which every individual who earns a CEH is required to swear an oath to uphold. For anyone who adheres to the original "Hacker Ethic" as described by Steven Levy in his book *Hackers*, several demands from the CEH Code of Ethics are very problematic.

To start with, item 16 of the Code states that one must vow "Not to take part in any black hat activity or be associated with any black hat community that serves to endanger networks." If we define "black hat activity" as illegal activity - although CEH does not - the first part of this seems reasonable enough. The second part raises some questions though. What is a "black hat community?" What if we are in a community where some of the members download illegal copies of episodes of *Game of Thrones?* Is this enough to warrant a violation? And beyond that, what if we are in a group where some people do "black hat" things, but we ourselves do not? Is it really fair to punish someone for the crimes of someone else, simply due to association?

It gets even worse with item 17, which demands us "Not to be part of any underground hacking community for purposes of preaching and expanding black hat activities." What do "preaching and expanding" mean? What if we're in an IRC channel where some people do illegal things, and we have discussions with them? Are we required to cut off ties with people? And who decides what constitutes "black hat?" What if we encourage civil disobedience, pushing to purposefully break a bad law in order to enact a greater good? Is this grounds for a Code violation? I now wonder if the hackers who devised Stuxnet, the worm that infected Iran's nuclear centrifuges, would be in violation of the Code, though they were carrying out orders from the President.

The last item we need to visit is a bit more controversial, but nonetheless important. Item 19 states that we should not be "convicted in any felony" nor should we have "violated any law of the land." This rule is simply too sweeping. What if we are a convicted felon for something unrelated to computers? And more important, what if we *are* a convicted felon, but have served our time, and want to reintegrate into society? If someone has done something wrong in the past and wants to redeem themselves, isn't agreeing to follow a set of ethics precisely what they should do? Why create a requirement that eliminates the very people who might want to use this certification to achieve that goal?

That's just the Code itself. And, while I think it is poorly thought out, the enforcement of it is even worse. The EC-Council, who provides this cert, has a procedure to report "violations" of the Code, found at cert.eccouncil.org/report-violation.html. The form amounts to filling out a police report, using the Code, and including the items we just reviewed as a pseudo-legal system. Anyone can fill out this form and report someone. It is in a sense creating secret police, because anyone who doesn't like us can figure out an interpretation of Code that will make us look bad. The result is that we could lose our certification. Of course, the EC-Council will likely assure us that these things would never happen and we're reading too much into their words. But then I must ask: what is the point of having a Code to which they force people to swear an oath if they do not plan to enforce it?

And it's not just that. More and more security and technology jobs these days have "CEH certification" as a job requirement, partly because it's a nice sounding term that HR can use to filter out resumes. So what happens when someone sees us download *Game of Thrones*, decides that this violates item 16, and reports us? If the EC-Council Tribunal takes up our case and decides against us, not only could we lose our certification, we could also lose our job and livelihood. And because this is becoming a standard with many companies, this amounts to being blacklisted from getting another tech job, unless EC-Council Tribunal, in their good graces, grants us some form of clemency.

Adding insult to injury, the use of the word "ethic" within the CEH Code is completely removed from any traditional definition. When we study ethics in school, we might have a class on Aristotle, or explore exercises like the Trolley Problem and learn that sometimes there is no good way out of a situation. With the CEH Code, all of the items reinforce a notion that mindless obedience to corporations [illegible] good, which betrays both the Hacker Ethic as well as a true exploration of the word "ethic." In truth, the CEH certification is a scheme that is used to trap people who are interested in working in tech into a situation that binds and controls not only what they do outside of work, but even the people with whom they associate.

To paraphrase Orwell, Big Brother is Certifying You.

Page 54 — 2600 Magazine

Introduction

Body

Conclusion

Autumn 2019 issue of 2600

Part two: getting from the first draft to published

- Rhetorical devices
  - “the art of effective or persuasive speaking or writing, especially the exploitation of figures of speech and other compositional techniques”
  - tool of persuasion
  - Robert Caro “On Writing”

Part two: getting from the first draft to published

- Flow - poetry

Once upon a midnight dreary, while I pondered, weak and weary,
Over many a quaint and curious volume of forgotten lore—
    While I nodded, nearly napping, suddenly there came a tapping,
As of some one gently rapping, rapping at my chamber door.

“The Raven” by Edgar Allen Poe

Part two: getting from the first draft to published

- Flow - short stories

The grandmother didn’t want to go to Florida. She wanted to visit some of her connections in east Tennessee and she was seizing at every chance to change Bailey’s mind. Bailey was the son she lived with, her only boy

“A Good Man is Hard to Find” - Flannery O’Connor

Part two: getting from the first draft to published

- Adding a “punch”

Happy families are all alike; every unhappy family is unhappy in its own way.

Anna Karenina - Leo Tolstoy

Part two: getting from the first draft to published

- Adding a “punch”

  Spring 2020 issue of 2600

Null-Routing Facebook: Using Small Tech to Fight Big Tech

by aestetix

I really hate Facebook. Part of this hatred is a general dislike of “social” media websites which pollute and destroy civil discourse with haphazard policies and elusive “algorithms,” but Facebook takes the evil to the next level. In this article, we’ll explore how they do this, and what you can do to fight back.

This evil began when Facebook got into the business of mass surveillance, starting with a website widget. According to them, we could add “one line of javascript” to our website, and it would magically enable people to like and share things like blog entries that we had written. This later expanded into other technologies, such as single-sign-on, where we could enable people to use their Facebook accounts to “log in” to our website and use our services.

But there’s something that Facebook didn’t mention. Every time a web browser makes a request to a website, it requests all the resources on the page, such as images, CSS, and so on. Including that “one line of javascript,” which makes a request to a Facebook URL and downloads javascript that enables the promoted functionality. And every time our web browser makes a request to Facebook, it creates a log entry on Facebook’s servers with all sorts of information, such as our user-agent and our IP address. For every website we visit that has this functionality enabled, Facebook can track us, even if we don’t have a Facebook account.

This is probably how Facebook collected the data that became “shadow profiles.” The public first learned about these through a public information request by Max Schrems in 2011 (details at `europe-v-facebook.org`). These shadow profiles - secret dossiers about people’s Internet browsing activities compiled without their knowledge or consent - have been the source of a lot of controversy, even coming up in Congressional and Parliamentary questioning, although Facebook refuses to address any concerns.

While the Internet was designed to route around censorship, it was also designed to route around surveillance. When the web browser requests an

Part two: getting from the first draft to published

- Ok, it’s ready, now what?