About this presentation

Digital forensics is a diverse subject area. Let’s talk a bit about the basics and then view the application of those basics through the lens of demos

Agenda

- About me
- The forensic process
- Fun stuff

Fall 2020

About me

whoami

Dominic Sellitto, CISSP

vCISO

About Me

Education:

- Bachelor of Science, Business Administration
- Master of Science, MIS

Security experience:

- Consultant/Senior Consultant, Cyber Risk services, Deloitte
- Lead Cybersecurity Consultant, Loptr LLC

Professional affiliations:

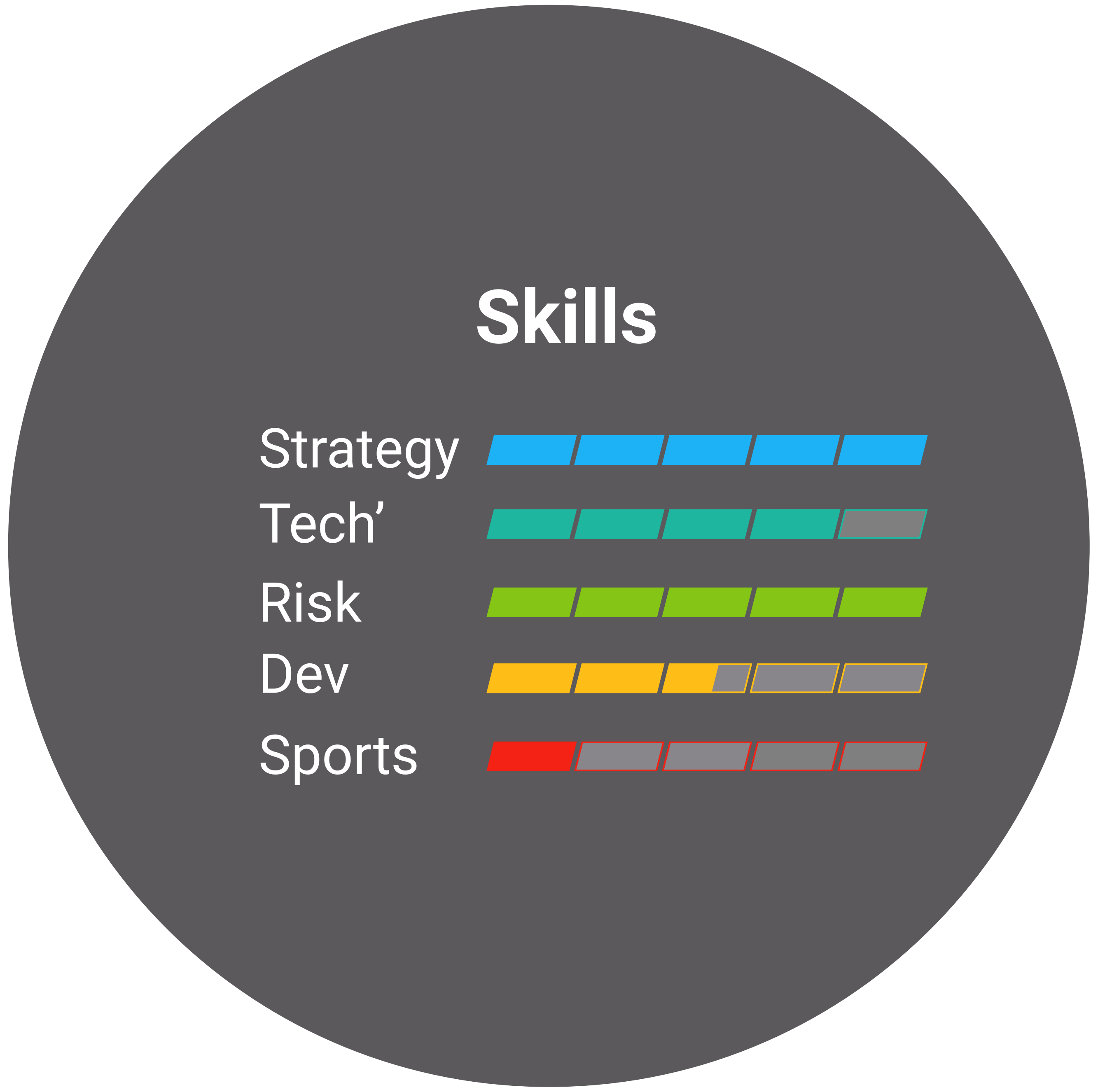
- ISC^2; Certified Information Systems Security Professional (CISSP)
- Buffalo Electronic Crimes Task Force

Publications:

- Vulnerability Assessment (ISACA, 2017)

Hats worn:

- Virtual CISO
- Project Manager
- Security Analyst
- Security Monitoring Analyst
- Security Architect



What is digital forensics?

Digital forensics is “the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data."

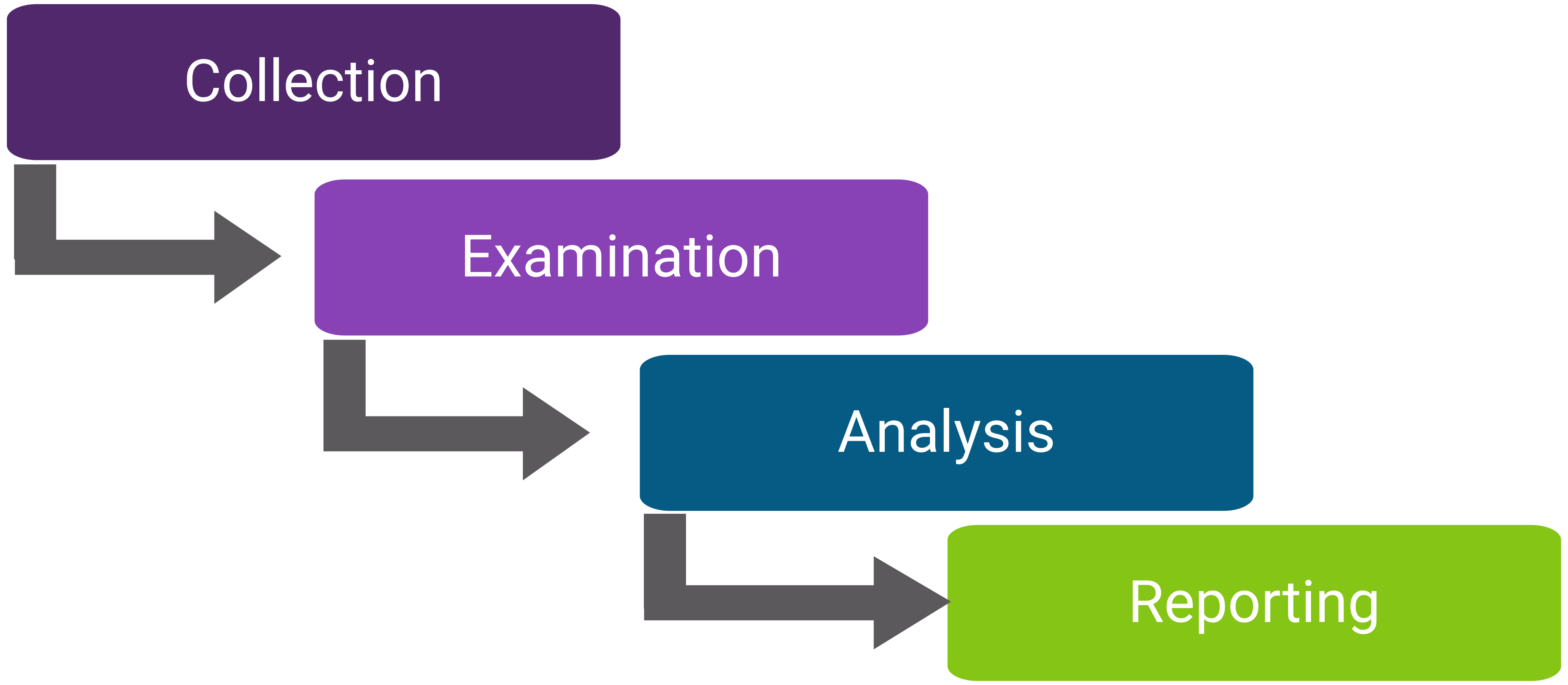
-NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response (Pg. 15)

Digital forensics may also be referred to as:

- Computer and Network forensics
- Data forensics

Phases of the forensics process

NIST 800-86: Guide to Integrating Forensic Techniques into Incident Response describes the 4 phases of the forensics process as follows:

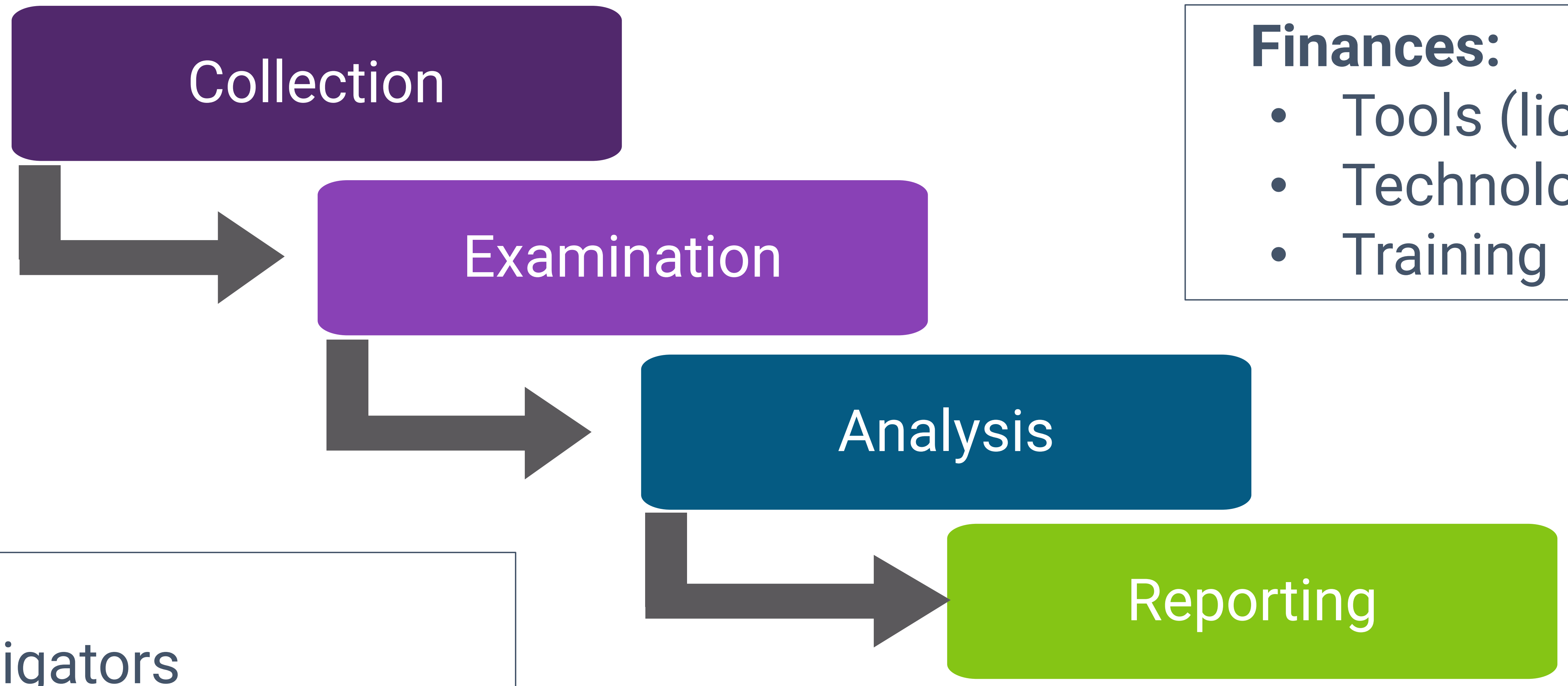


Source: NIST 800-86: Guide to Integrating Forensic Techniques into Incident Response

Enabling factors

In order to repeatably execute the process, you need some things…

Governance:
- Policies
- Procedures
- Standards



Finances:
- Tools (licensing)
- Technologies
- Training

People:
- Investigators
- IT professionals
- Incident response team
- In-house vs. outsourced

Location:
- Lab / room
- Access control
- Monitoring

Source: NIST 800-86: Guide to Integrating Forensic Techniques into Incident Response

Forensic areas of practice

You might just think of forensics as examining hard drives, but it’s much more than that:

Media forensics

Malware analysis

Memory forensics

Network forensics

Mobile forensics

Cloud forensics

Email forensics

Digital media manipulation

IoT forensics

Automobile forensics

Network forensics

Packets contain all of the information being sent across a network, including the source and destination machine, protocol being used, and the actual data being sent.

Network logs are records of network events— they tell you that something happened over the network (like source, destination, protocol) but do not contain the actual data that was sent.

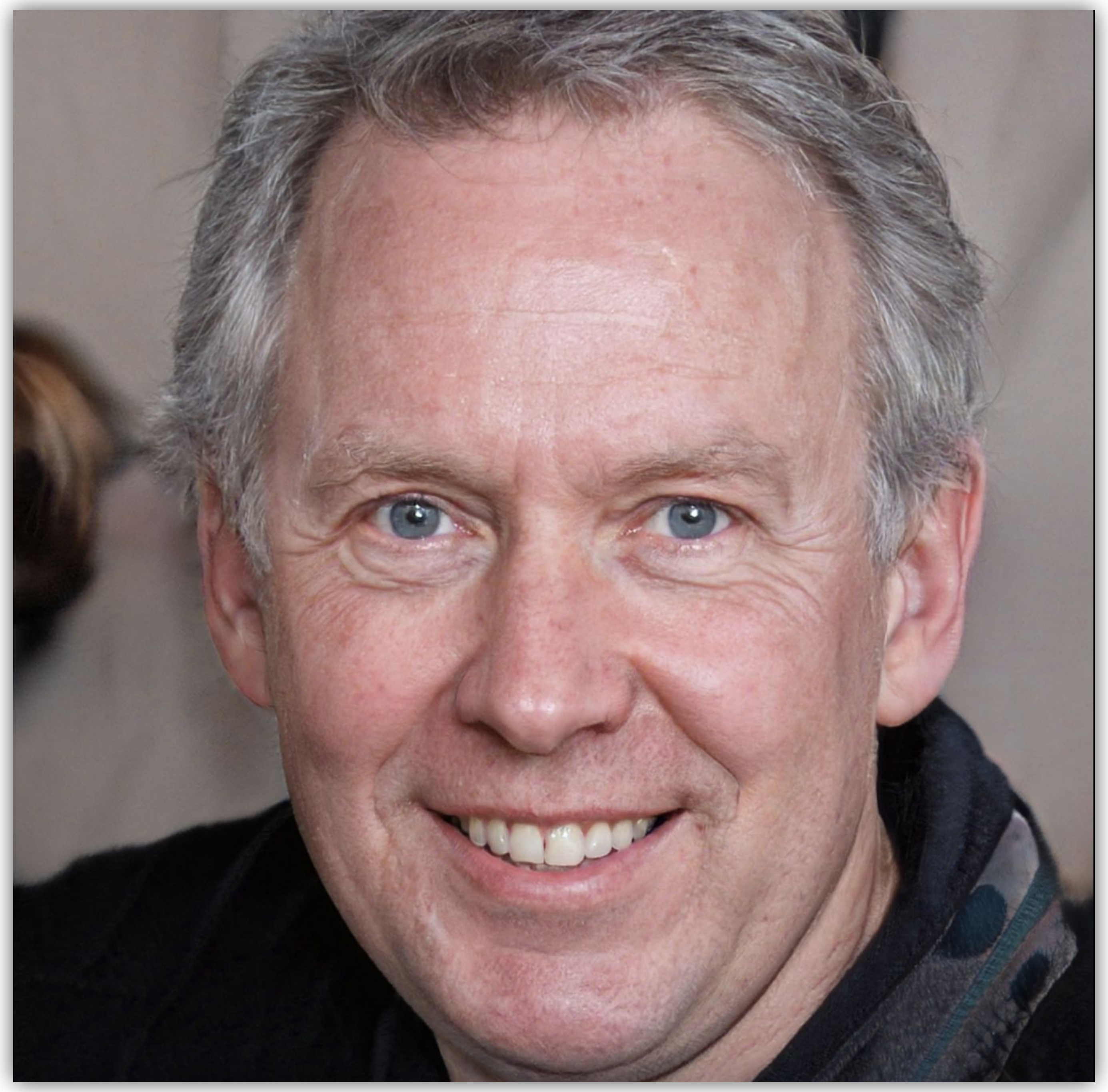
Introduction to digital forensics

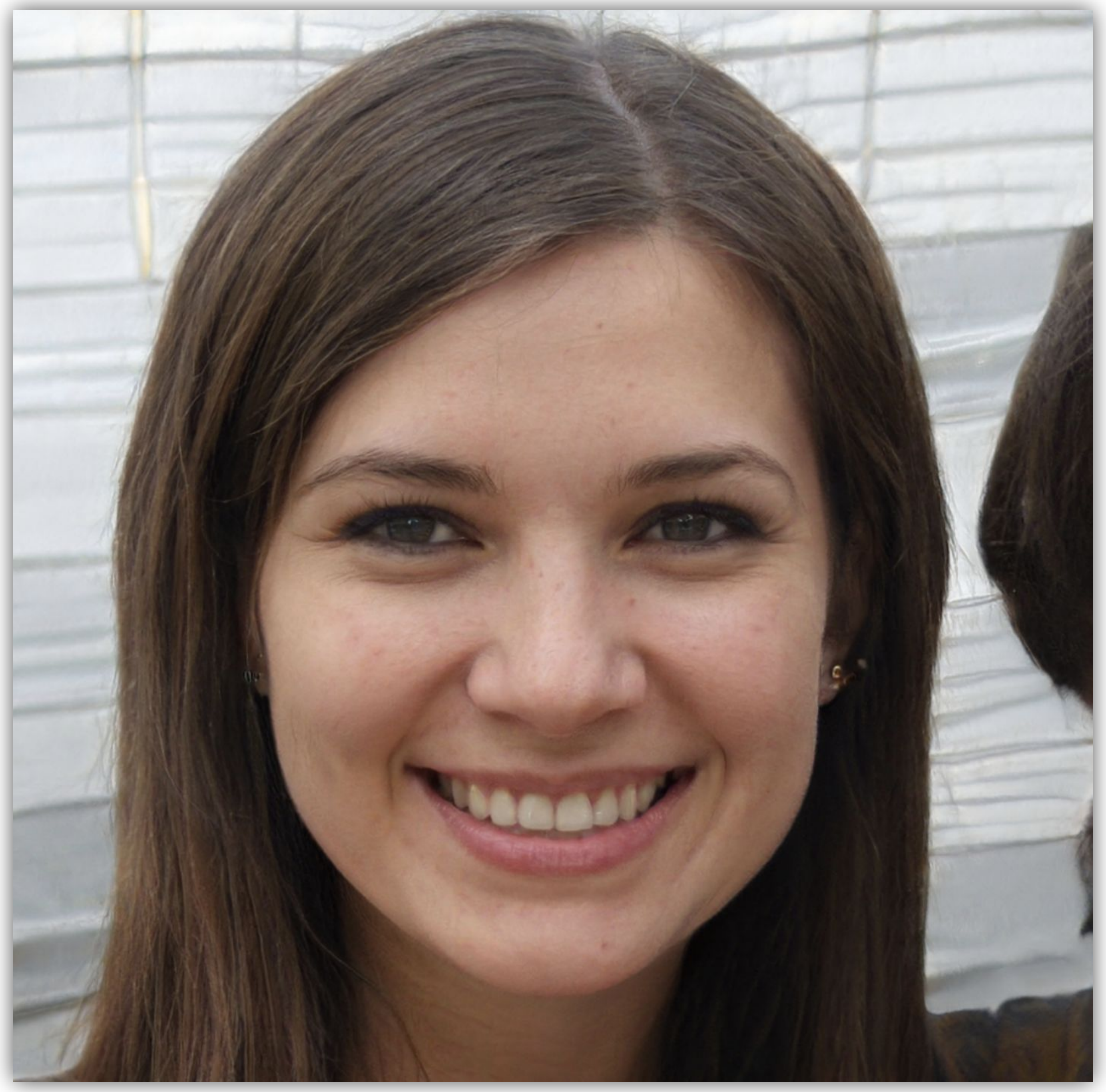
Network forensics: Wireshark

Let’s talk about Wireshark…

Digital media manipulation

Which of these is fake?





Malware analysis…

What’s that program ***really*** doing?

Email forensics…

Oh look, a **phish**!