TEST SECURITY TOPICS

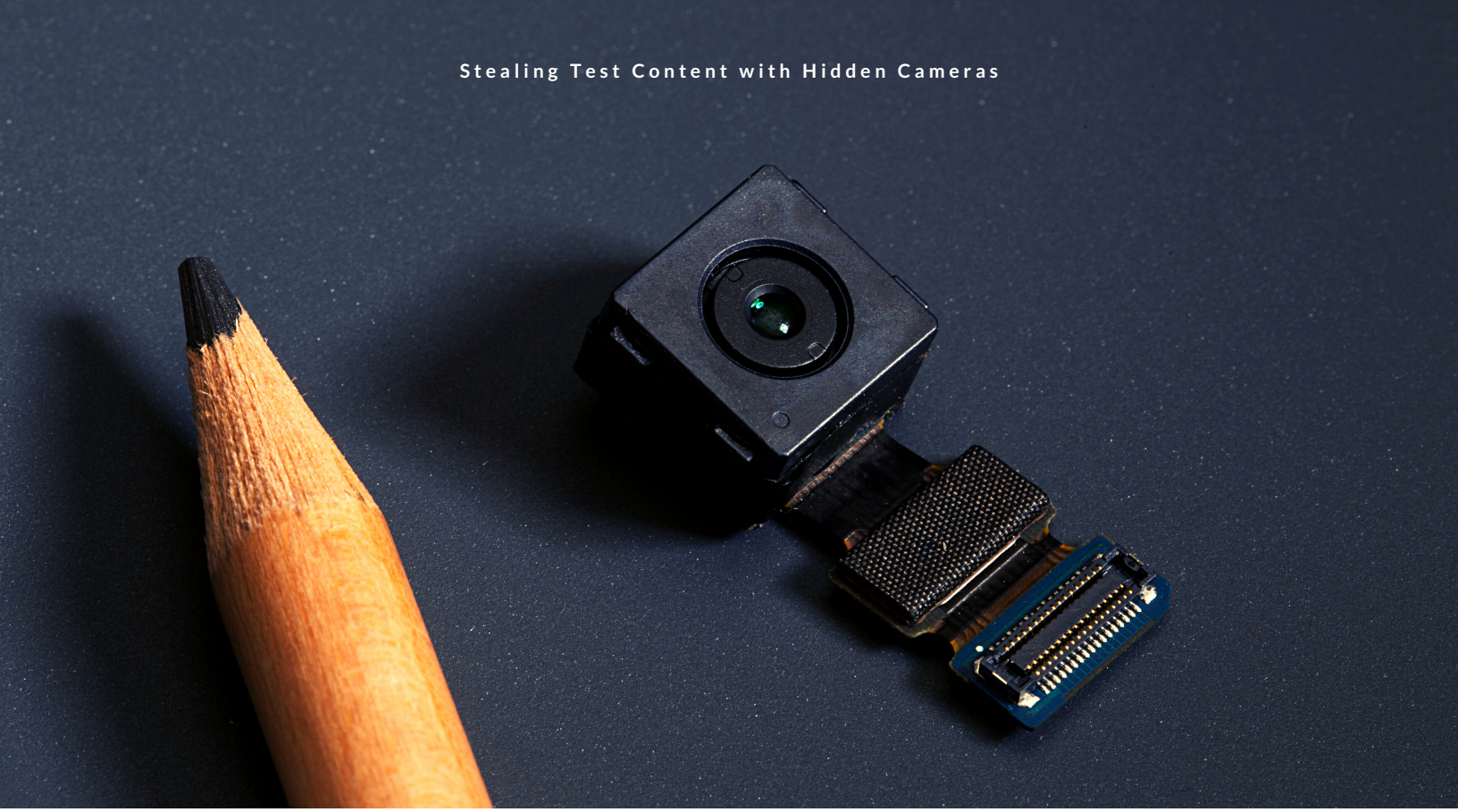
STEALING TEST CONTENT WITH HIDDEN CAMERAS

SOMETIMES TO CATCH A FRAUDSTER, YOU HAVE TO THINK LIKE A FRAUDSTER.

DR. CHRISTOPHER FOSTER
AND ANDREW MARDER

2021

CONTENTS



LIGHTS, CAMERA, TESTING.

Cheating and test theft take many forms in the testing space. All have been affected in one way or another by the growing accessibility and lowered cost of high-tech tools that make cheating easy, affordable, and almost undetectable.

In this white paper, we've donned our technological black hats to peer down at the level where the fraudsters play and understand their games. First, we'll discuss the power, affordability, and accessibility of modern hidden cameras. Next, we'll show you just how easy it is to use hidden cameras, even (and almost especially) when a proctor is present. Finally, we'll talk about ways you can make it more difficult for these methods to work.

In this white paper, we will not be revealing anything that fraudsters don't already know. It may be uncomfortable to stoop to their level and explore our own vulnerabilities, but it's the only way we can beat them. Let's dive in:

Cameras are categorized into three different areas: Hidden objects, small and disguisable, and wearable.

HIDDEN OBJECT CAMERAS

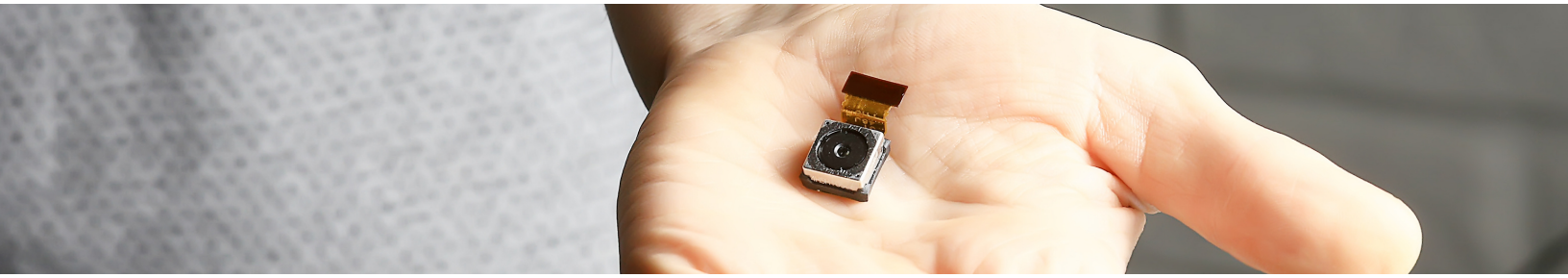
You can find hidden cameras in almost anything these days. Cameras come in alarm clocks, power adapters, wall hardware and hooks, paint cans, USB ports, oscillating fans, you name it. These types of cameras operate using an outlet but can come with a backup battery. Even when they're not plugged in, the battery can last up to two or three hours.

SMALL AND DISGUISABLE CAMERAS

Small and disguisable cameras are just regular cameras that are very small. The advantage of these mini cameras is that they can be disguised or hidden as other things. At a low price point, you could buy this camera (FIGURE X), which is about half the size of a nickel. Disguisable cameras can pose as bottles, coat hangers, you name it. Like above, these types of cameras operate using an outlet, but they can also come with a backup battery. If they're not plugged in, the battery can last up to two or three hours.

WEARABLE CAMERAS

Hidden cameras that you can wear on your body are of particular concern to test programs that administer exams in testing centers. In fact, many test centers are on the lookout for examinees who are wearing wearable camera watches, keys, earphones, pins, buttons, or tie clips. Dozens of different types of hidden camera watches exist on the marketplace today, but there are surely more types of wearable cameras we aren't even aware of. In addition, most wearables are powered by battery—but their lifespan is low, lasting only one to two hours. This means, in theory, that if a test is very long, the battery of one of these cameras may not last throughout the entire exam.



PRICING

Button Cam	$30 (Including Amazon two-day shipping)
DVD Case	$299 (More advanced)
Monster Energy Drink Cam	$319 (can last for several hours on battery power)

STORAGE

These cameras all need to store data. There are a couple of basic ways to do this. The first is using Wi-Fi. Many of the wearable cameras broadcast on Wi-Fi signals, which you can connect to with a phone. In this scenario, the camera needs the phone itself to store the videos.

Many devices, if they're Wi-Fi-enabled, can connect to any wireless network and simply upload everything they record into the cloud.

Larger cameras almost always have some sort of local storage, such as an SD card. A 32-gigabyte mini-SD card costs about $9, fits in most cameras, and can hold two hours and 45 minutes of video in 1080p. So for just a bit more money, a person could contain nine hours of video and record entire test sessions with no problem.

Figure 1 explores the different camera resolutions, including 1080p, 4k, and more. However, here's what you need to know: for the purposes of harvesting exam questions, the quality of the camera doesn't matter. Most cameras can pick up a readable graphic on a computer screen from across the room. Even if the camera resolution happens to be very low, a simple zoom in and font adjustment will fix the image in many cases. So, unfortunately, even the cheapest cameras will be able to easily grab content from a screen.

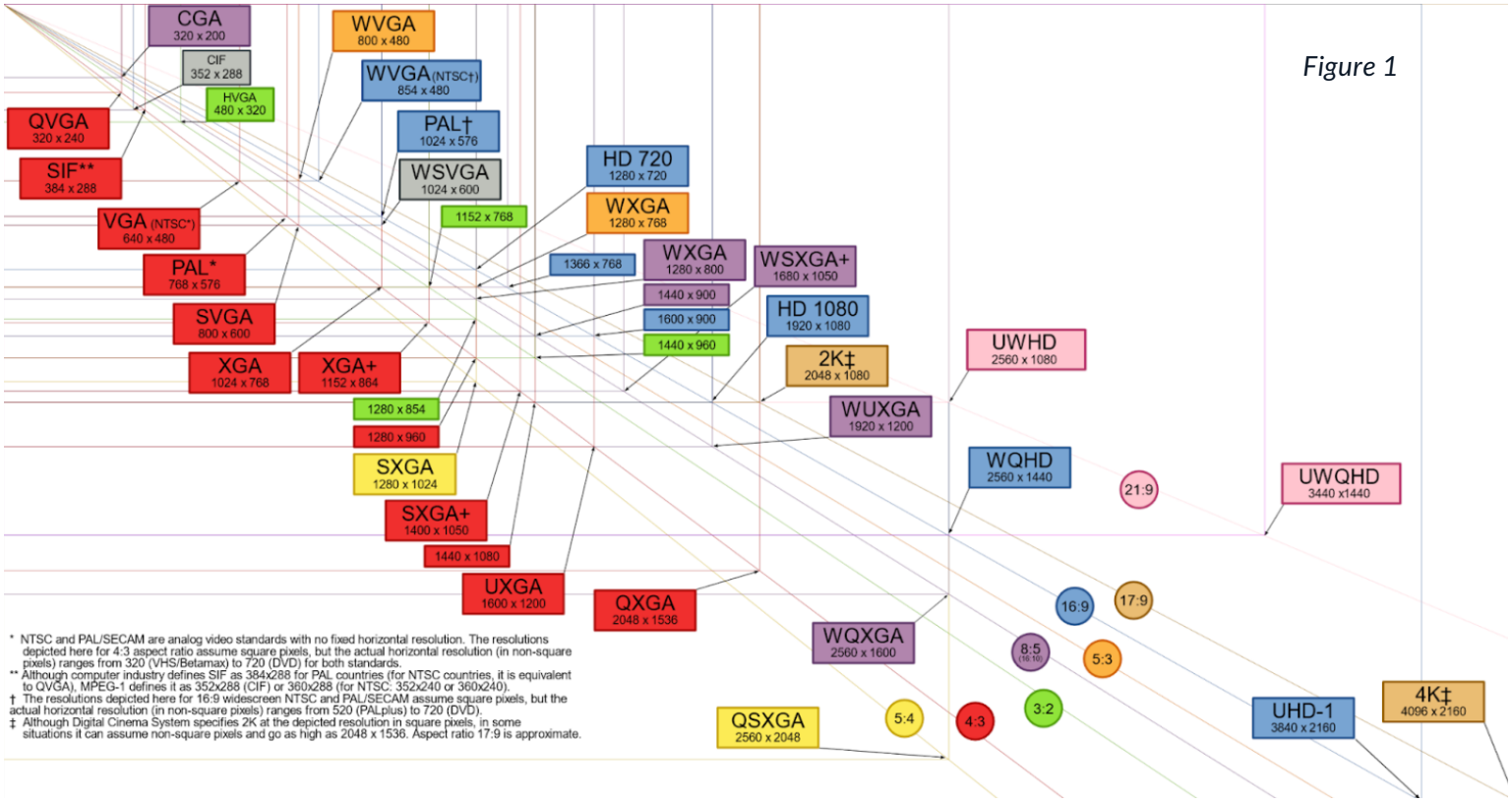


Figure 1

IS DETECTION POSSIBLE?

How do testing programs detect these hidden cameras? If there are so many different variations, what are you supposed to look for? It's not easy, especially since these cameras are designed to be hidden. However, there are a few things you can look for:

UNUSUAL LIGHTS

Most small wearable cameras (like watches, eyeglasses, and buttons) will use lights to communicate their functionality in the absence of an LCD screen. This means they'll use different communicative "blinks" to tell you what they're doing. For example, a red blink may indicate that the camera has just stopped recording or is out of memory. A slow, green blinking light may mean that the camera is recording. A yellow light may mean that the battery is low. The point is, there needs to be some form of communication between the wearer and the device, and lights are a common way to do that.

STRANGE OPTICS (REMOTE)

Does anything seem out of the ordinary? Small holes in walls, wires where they shouldn't be, or light reflections coming off of hidden lenses, for example?

PHYSICAL DETECTION (IN-PERSON)

You can use a special device to detect radio frequency broadcasts. You can also use metal detectors to detect wearable cameras. However, these methods of detection are only effective in in-person settings and can only be done if you have the time, equipment, staffing, and budget. An examinee taking a test at home with an online proctor will likely never have to worry about being detected this way.

CAN YOU SPOT THE HIDDEN CAMERA?

Here is an image of Christopher looking at his screen, which has test material on it. Can you spot the hidden camera?

Well, actually, it's cameras—plural. How many? **Five**.

1. One is hidden inside the roll of paper towels.
2. Another is peeking through the cardboard that is lying in the window.
3. A third is a wearable hidden camera, hidden in the button peeking through the shirt (Notice that this is virtually undetectable, as he is wearing a black shirt).
4. A concealed cell phone made it to the party as well. Its camera is peering through a hole that the examinee simply poked in some Styrofoam he had lying around the house.
5. Finally, a GoPro (not even hidden) is sitting on the shelf in the background. (Notice how difficult this is to see on a standard computer webcam).

What's more troubling? There's more here than meets the eye (and we've just established that "what meets the eye" is still pretty hard to see). There are three additional cameras in the room, all with clean shots of the screen, and all virtually undetectable in a proctored room sweep. Because of the webcam's limited field of vision, these cameras are "off-screen," and would likely be missed during a sweep of the room. Why? Because room sweeps are typically focused on looking for additional people in the room, illicit materials in the workspace, and other more obvious things.

Let's look at these cameras. Up on the right platform, there is a very nice camera pointing directly at the screen. On the top left, where you cannot see, is the home camera Chris uses to watch his dogs when he's away. Then, directly below the webcam, Chris has taped a button cam from Amazon that can collect everything on the screen without being detected by even the most thorough room sweep.

OUTRANGING

Infuriatingly, a standard webcam has a sub-par lens and can only film in 1080p. A GoPro, on the other hand, can film in 4K. So, all the examinee needs to do is put the high-fidelity camera far enough away from the low-fidelity camera that it can't easily be recognized, while still being able to get a clean shot of the screen. That, unfortunately, is not difficult to do.

In this case, the GoPro is up on a ledge getting a perfect shot of the screen, and it cannot be recognized by the webcam. From that distance, the GoPro will still easily capture quality footage of anything above a 10-point font.

How much would it really cost to harvest a series of items from a test? Referring again to Figure 1, all five hidden cameras cost less than $100 total. However, in most cases, examinees can use the technology they already have on hand (cell phones, home security cameras, GoPros, and more) to commit this type of fraud.

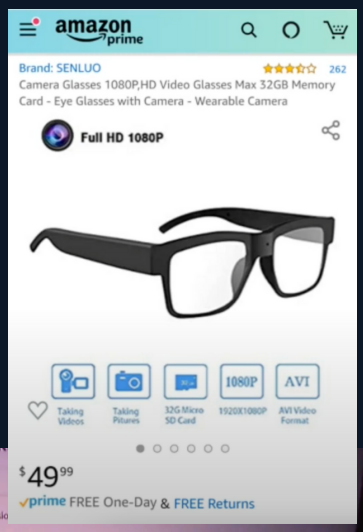
LET'S LOOK AT A FEW MORE EXAMPLES...

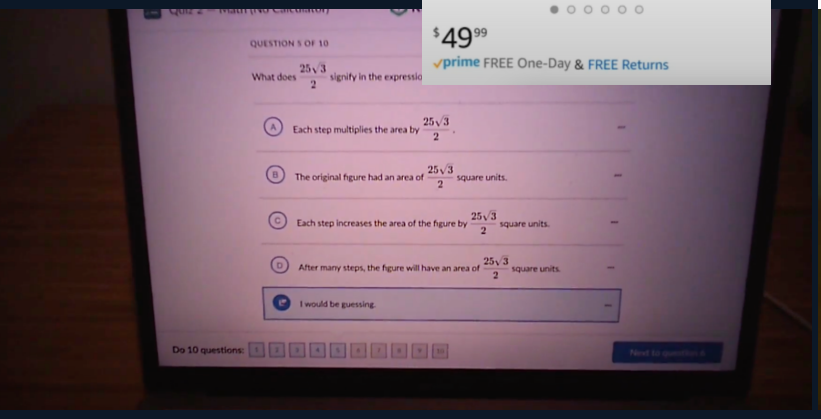
CAN YOU SPOT THE HIDDEN CAMERA?

Here is an image of Andrew looking at his screen, which has test material on it. Can you spot the hidden camera in this photo?

It's on the bridge of Andrew's nose.

These hidden camera glasses were purchased from Amazon for just under $50. They work like a charm—capturing all the text, graphics, mathematical notations, and whatever else an examinee would need to copy the content of an item.

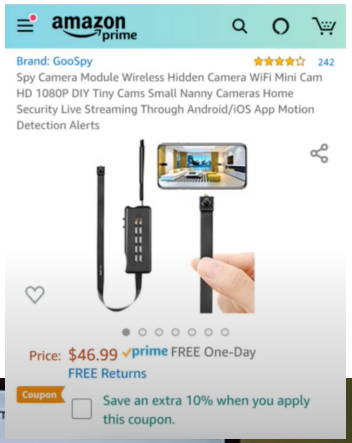


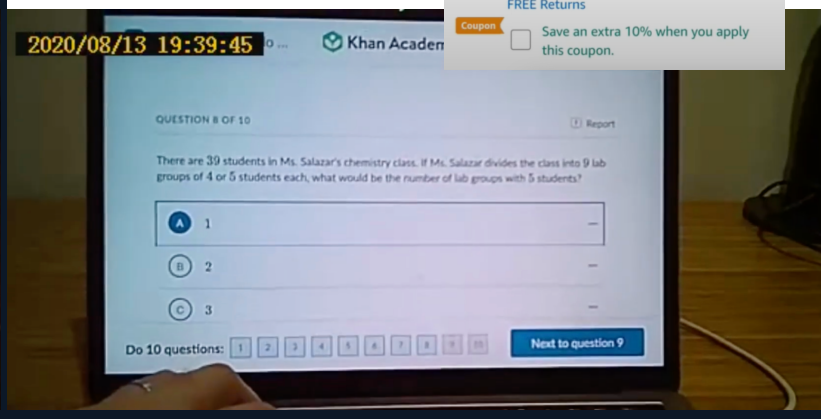


Here is another example of Andrew looking at his screen, which has test material displayed. Can you spot the hidden camera in this photo?

Like before, Andrew has used a dark-colored shirt to disguise a camera. This time, it's taped to his chest.

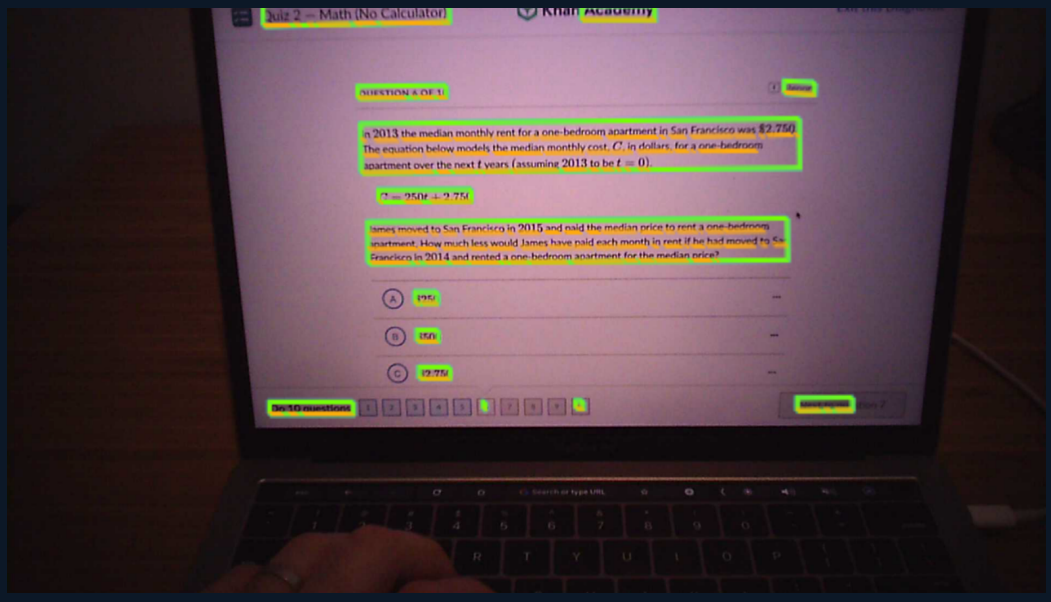
On Amazon, that camera goes for $47 (and Andrew got a 10% off coupon, too). The camera broadcasts a Wi-Fi signal to send real-time images to a smartphone app that displays all that's being recorded.





To test the hidden cameras, we recorded practice SAT questions from Khan Academy. The glasses were effective when the browser was zoomed to 150%. The hidden camera taped to Andrew's shirt was effective when the browser was zoomed to 200%. Both tests were done on a 13-inch laptop. Both cameras can capture all the text, images, and mathematical notation, making it sufficient for stealing test content. The glasses have a slightly higher-quality camera, but the second camera was easier to conceal.

Suppose a thief records a test session. How will they convert that video into text for wide distribution? Cue artificial intelligence. Andrew took one frame from the glasses camera and fed it into Google's Vision API, and overall the results were extremely good.



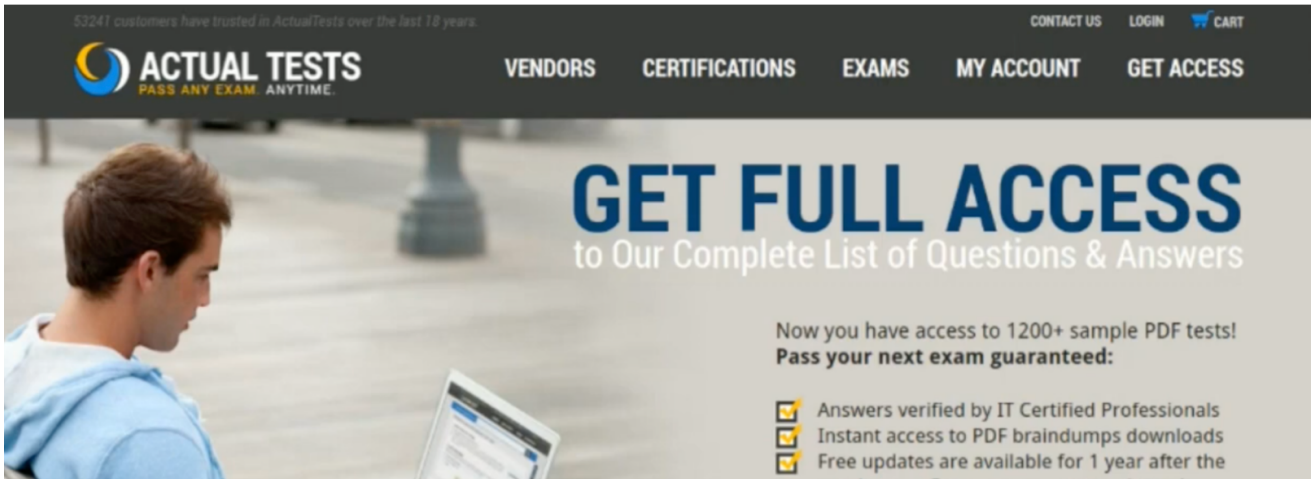
Google's Vision API recreated the text quite well. The green boxes indicate the text that the API recognized. All the text is correct, but the equation is not quite right. There is text around the page that is recognized as well, though that text isn't part of the test question. There are going to be slight mistakes coming out of AI. It would be difficult to handle questions that span multiple frames, but overall, this would be a feasible way to extract text from video content.

EXPLORING BRAINDUMPS

Hidden cameras capture this high-quality test content for no shortage of potential buyers. Generally, braindump sites are the final destinations for this kind of stolen IP. A braindump is a website that actively steals live test questions and then resells them. Typically, a braindump site will accept stolen IP from anyone. Some braindumps even hire subject matter experts to correctly score the exam items, just to be sure clients get what they're paying for.

Potential examinees can then purchase complete live exams at a relatively low cost. Once this happens, it immediately calls into question the validity of any exam score given by a specific testing program.

Here's an example of a braindump ad:



This braindump site advertises actual tests. You can pass any exam at any time. They claim IT professionals have verified their answers and that the questions are always up-to-date. Some sites advertise thousands of different exams, many for as low as $20.

The sad reality is that most IT tests can be found this way. The higher the stakes become, the more incentive there is to steal. Browse through the news and you'll find this phenomenon holds true in K-12 testing, higher education, certification testing, medical licensing, and other industries as well.

WHAT'RE THE SOLUTIONS?

There are two main preventative approaches. The first is the reduction of content exposure, or revealing only a small fraction of the test content to each test taker. There are several methods to achieve this, including multiple test forms, computer adaptive testing, linear-on-the-fly testing, automatic item generation, SmartItem™ technology, and Discrete Option Multiple Choice™ (DOMC) items.

On the detection side, watermarking is a valuable way to identify exactly who has stolen any given test content. Watermarking is useful and compelling as proof in legal situations as well. A bonus to this approach is the ability to publicize that your exams are watermarked, which can reduce theft and fraud by deterring would-be cheaters.

CONCLUSION

WHAT SHOULD WE KNOW ABOUT HIDDEN CAMERAS AND TESTING?

The information in this paper represents a rude awakening: stealing your test content is more accessible and less detectable than ever before. Hidden cameras are a significant security threat. It is very difficult, especially for online proctors, to locate any hidden cameras. High-stakes test questions are valuable, and bad actors can profit from selling that content. Instead of relying solely on proctors, testing programs must adopt preventative measures and measures that detect and deter the clandestine capture of valuable intellectual property.