Module 2 video 3: Verifying Images and Videos

[00:00:00] Alright. Welcome back to week 2.

[00:00:03] We are in our final lesson, which is Verifying Images and Videos. I'm really excited to show you guys all the stuff that we can do. This is one of my favorite approaches to verification.

[00:00:16] So this lesson will go over what to look for when verifying images and videos. We're also going to look at the different reverse image options that we have, as well as detecting GAN-generated images, video search using Invid and WeVerify is going to be a big focus, as well as looking at shallow fakes and deep fakes and the different verification approaches for both.

[00:00:41] Just as a note. This lesson will have a lot of examples. So just be ready to open them up. All right. Let's get to it.

[00:00:48] So what to look for in images and videos? I always like to remind myself to know the weather. Know the weather the day that I'm looking at. So what does this mean?

[00:01:03] Every video contains a few different details inside of it. It contains the people. It contains the setting. It contains little clues that we can look for. And when I say "know the weather," I mean, one of the best things to know and to understand about the video that you're looking at is when was it shot? If other videos from that event show snow, rain, cloudiness, not a lot of leaves on trees or not a lot of plants in the ground. But the video that you're looking at is the opposite. That's your first clue that something is wrong. So take a moment and place what it is that you're looking at.

[00:01:48] Take note of any street names, logos, car plates, transit. Are there any landmarks in the image like buildings or bridges, statues, mountains in the distance that maybe you could use as a jumping off point? Does it look fake or does this speech contain unusual patterns? Does something just feel off to you? And don't put that feeling aside. Listen to that feeling. And if you're reporting on a location that you haven't been to before, use Google Street you to familiarize yourself with what it might look like.

[00:02:24] So let's look at a context clue example. Here's a video that during the Black Lives Matter protests, somebody tweeted and said, this video's from Minneapolis. And it clearly shows one of the protesters dragging an A.T.M. onto a car. And they use this video as a sort of proof that that protesters are mean spirited, that they are not there for the cause, but they're there for personal enrichment.

[00:03:04] OK, let's watch this video very quickly.

[00:03:27] You got to admire the dedication.

[00:03:31] Alright. So I'm just going to pause the video right here and I'm going to point you to what I think are some really interesting clues. So what is the road itself? You can kind of. Well, you can kind of see that there's like a bike lane here. So if we wanted to sort of figure out if Minneapolis has bike lanes. We could do that.

[00:03:54] But our number one clue is actually right in front of us. This bus says NJ Transit on it. So if we open up Google and search NJ Transit. And maybe type in bus. We can go to images and look at a bus that seems to have a matching logo.

[00:04:22] This is a pretty concrete way to look at a video and say there is no way that this was filmed in in Minneapolis, because the bus itself has NJ Transit, which means it was filmed in New Jersey. This is just one example of how a context clue can really save you the time of verification.

[00:04:48] Alright, let's get back to it. So reverse image search is a really basic tool that can be made incredibly powerful. And that's because every search engine has a different strength and different weaknesses.

[00:05:03] This chart that was compiled by DomainTools is a really great comparison of what certain what what each search engine is good at.

[00:05:15] So the first thing that you should do when you are looking at an image is to isolate the image in a new tab. That way you'll get the full picture and you'll get a sort of higher quality image. And you can do that by just right clicking and selecting open image in a new tab.

[00:05:33] Let's try this with one image and see how the different search engines behave. And as a note, you should have the InVid plugin installed already. If you don't, then just follow along for a second and I'll shoot you a link in a moment.

[00:05:57] So let's look at this photo and let's say we are very curious to figure out who is in this photo. So our first step should be to right click, open image in a new tab. So this allows us to sort of isolate the image. It looks like it wasn't previously cropped, but now we have it in front of us and we can see the image if we like. Now, let's right click and go to our InVid WeVerify plugin and select reverse image search for Google. Alright. Trump family at convention last night. Great, great. There is the week report. So we see this image, we sort of see other images like it. And that's about as much as we can get out of Google.

[00:06:57] Now, if we search this image on Yandex. Which is the Russian search engine. It will first of all, it's unfortunately in Russian, so some of this stuff you might need to use Google Translate for. But it will also give us other versions of this picture. Now, Yandex is particularly good at facial recognition. So if you're looking at a profile photo of somebody, that's, definitely, Yandex is your engine. Yandex is your Google engine. In this case, it's pretty helpful. It's showing us sort of other pictures from the night, but it doesn't give us a way to figure out, okay, who is in this photo.

[00:07:43] So let's go back to our image once again and just right click it one more time. And in this case, select Bing. Now you will laugh but Bing is by far one of my favorite search engines for this one key function, because it already, if you can see, identify that Eric Trump, his girlfriend, Kimberly and Lara Trump are all in the image. Now because Bing has already done the work for us. It's pretty clear that we already understand who we're looking at. But let's just go and see if we could have gotten this information another way if Bing wasn't helping us. So right here on the on the bottom, you will see on the bottom left you'll see visual search. And I want you to click that.

[00:08:32] Visual search will bring up a little box that you can use to zero in on people in the image which will then show you who it is you're looking at. So here we clearly see. We clearly see other images of Eric Trump. We can see his girlfriend, Kimberly, very clearly come up, as well as other images of her.

[00:09:06] And we also see that if we put this box over another face, Lara Trump comes up. Now, this is not perfect. If we put this box over Donald Trump, Junior, it's a miss because it's in a profile and profiles are much more difficult for search engines at this point. And the same goes for Tiffany Trump. Unfortunately, not much usefulness in the results there.

[00:09:33] But this should give you a pretty strong idea of why these different search engines are handy and how you can use them all in your investigations and in your verification.

[00:09:48] Now a quick note on GAN generated images, which is computer generated images. They are still imperfect, but they are pretty effective. Usually we see them a lot in fake profiles where people set up a fake persona online and use a computer generated image that can't be easily reverse image searched back.

[00:10:11] So what do you do in that situation? Well, remember to isolate the image so that you have the full picture and then look for little imperfections. Look for little things that regular normal human beings would not have. So this is like bleed on hair or ear lobes. Look for small details like teeth, eyebrow and hairlines. Symmetric details like glasses and earrings are also extremely imperfect at this moment and background issues you can also very clearly see that usually backgrounds are just a little bit washed out. They look a little bit strange.

[00:10:52] One more fantastic tip that researchers found is that GAN generated images all have features on the same place and along the same access. So a computer generated image will generally follow the eyes being in the same place, the nose be in the same place, the mouth being the same place as you can see in this image. Whereas regular photos that researchers analyzed, they don't have that same issue. So look for those consistencies as well.

[00:11:27] So I'm just going to show you a quick Web site that will help you train yourself so that you understand what GAN generated image looks like and what to do when it comes up. So this Web site is called WhichFacesIsReal. And it sort of, it allows you to come, it compares computer generated images with human images. So here you can select one of the images. I thought this was the computer generated image. And I was right. But I didn't click on the wrong things. So let's try this one again. So choose the person who is real so we can see here around the eye. There's a little strange imperfection going on and around the ear as well. Something is happening strange here. This neck is a little too straight. It's not shaped quite right. So once again, this one looks to be the real image.

[00:12:33] So you can use this Web site to go through a few of them. Some are harder, some are easier. And that way you'll get used to looking at computer generated images and you'll get a little bit better at detecting them.

[00:12:46] Alright, so for video search, this is gonna be another demo. Video search has always been tricky, but we have one fantastic tool that really helps us figure out what's going on here. You can download the WeVerify extension at bit.ly/video-ext. And I'm also going to wait a second for you guys to open up the video and the image example that I would like for us to take up. So just take a moment to do all of that now. Pause the video if you need to. Before we move on to the next demo.

[00:13:22] Alright, so let's open up our video and take a quick walk through how WeVerify can be useful to us in this situation. So I just want you to copy the tweet that that we have here, copy the url and click on the analysis tool in your Invid toolbar. Now, if you want, if you need to, open up the image toolbar, it's going to be right here up with your Chrome extensions. You can just click open Invid.

[00:13:59] Great. Here we go. So paste the URL in here, this works for all major social media networks. And click submit here. What it will do is it will give you as much information about this video is publicly available all in one place and it will give you the duration of the video. How many likes it's gotten, how it was uploaded, related hashtags, related people that were mentioned. There is the thumbnail for the video. If you need to click on it one moment here. There it is. You can converge this through a time converter, but this is when the video was uploaded.

[00:14:45] But here's the best part. Because, because we cannot reverse image search video on Google. What we can do instead is search the thumbnails for the video. So in this case, for example, this the claim is that images launched by Iran were shot down, the artilleries using an artillery system. This is once again going back to our initial example to the Iran attack and Qasem Soleimani killing. And what you can do is what WeVerify and Invid allow you to do is essentially search the thumbnail for the image to see where else it could have come up.

[00:15:34] So we can just go ahead and click on it and then select. Let's go with Google Image Search for this one.

[00:15:46] So right away, we can see that the words associated with it are Israel, not Iran. And we can see that this video has been used many times before. Now, this is actually enough for us to debunk this video. We can see here that it was uploaded October 23, 2019, whereas the attack that we're talking about happened in January 2020. This posts is from January 8th 2020.

[00:16:14] So we can we can already say that, no, this is false.

[00:16:23] And actually we can see the tweet that we were looking at crop up here.

[00:16:29] But because it suggested Israel to us. Why don't we. Why don't we type in the word Israel and see what happens.

[00:16:43] So the handy thing with Google is that it does allow you to search for keywords alongside your image so you can try different combinations, just like you would with the Twitter search to see if anything interesting will come up.

[00:17:03] So in this case, we once again see the tweets that, the tweets that we were looking at previously. So this wasn't particularly helpful for us. So why don't we go back to our previous search and just click on the first result that Google suggested to us?

[00:17:28] Fantastic. So here for the context analysis, we're getting the same landscape. It looks like it's the same lasers. And once again, this video was uploaded on September 4th, 2019. So we can very easily see that this video is not from the Iran missile attack.

[00:17:47] There are a few other features that Invid has that are extremely handy. And the one that I really want to show you is keyframes. So let's just pop the url back in here and click submit.

[00:18:03] So what this will do is this will break down the images that are used in the video. So in this case, if you wanted to isolate an individual image, you could right click select the Invid, verify option. And you can look at the magnifier. You can search all of the search engines and you can look up image forensics of that, something that you're familiar with. So, for example, if you choose the magnifier, it will open in a new window. And now we can use our mouths to scroll in and out of the image. This is very handy for when we need to see particular details.

[00:18:48] So that is image. That is video search. But Invid is equally as useful for image search. And I'd like to show you one particular use case. And that is going to be under the invid-ex2 url that I gave. It should open up to this page right here.

[00:19:12] Now, this page has been spreading false information about Kamala Harris. And I would like to understand what this birth certificate is. So I'm going to right click and I'm going to once again open the image in a new tab.

[00:19:26] Great. So this gives us a larger version of this image. And once again, you can either. Right. Click or just copy the url here. I'm going to right. Click and say copy, image address.

[00:19:39] Now, let's go back to our Invid extension and click on the metadata option.

[00:19:48] Let's paste the url in the in here. And you can also upload the image, if you like, and click submit. Fantastic. So Invid is reading the data that was attached to this image, which social media networks scrub. But if you find an image on a Web site, you might look out and see the metadata.

[00:20:12] In this case, we have a name associated with this image. Tyler Wells, which also happens to be the woman who runs the Web site. And you also have the create date for the image, which is 2019. So dropping in an image into Invid can be really helpful. We can also use the magnifier on that image. So I'm just going to click submit here, paste that image. And if we needed to zoom in on any details here, it would allow us to do that, which is very, very handy.

[00:20:52] So this is Invid a really powerful video tool.

[00:20:57] Now, let's quickly talk about Shallowfakes and Deepfakes.

[00:21:02] A shallowfake is an unsophisticated, manipulated video that can still be extremely effective.

[00:21:09] This can include an audio change, slowing a video down or substituting it for another image. Here's a quick example of a shallowfake that we can all take up.

[00:21:24] That qualifies you for this job.

[00:21:26] I was growing up during the Clinton era. And then basically when I was in middle school, 9/11 happened.

[00:21:36] So this image, this video, rather, was published online under the guise of a joke, and it's stitched together to separate interviews that that took place. So one is an interview with Alexandria Ocasio-Cortez. And one was with a host of right wing news channel.

[00:22:00] So why don't we pop this image into WeVerify and see if we can get some different frames from this video.

[00:22:11] So what the keyframes will allow us to do is they will allow us to look at different portions of the video at different times. So this way we can reverse image search a few different things within the video rather than searching only the thumbnail itself. So this process can take a hot second, but let's give it a try. Anyway.

[00:22:41] OK. So now what this did is it gave us all the different shots within the video that we can then reverse image search and we can also download all of these if we need to.

[00:22:53] So I'm going to go ahead and pick the first one and just right click. And once again, I'm just gonna go with Google on this one. So. Right. Click and search Google for image. So immediately the the thing that comes up is girl rather than Alexander Ocasio-Cortez, which is who we're looking at. So why don't we just type in AOC to see if that will help us with the results? Alright. So we're still getting a lot of memes.

[00:23:29] And how about we do AOC interview? Alright, great. So now we're getting a little bit better results and we're getting this image here, which doesn't actually look like it came from the shallowfake video that we just watched. So by clicking on this, we are seeing the similar image. This is clearly we're seeing the same wall, the same outfit, and we're seeing a lot of different images from this same interview. We can see the same wall in the same outfit here. So let's go ahead and click on one of the links here.

[00:24:21] And looks like the result is actually the fake interview, the coverage of the fake interview, which is just as handy. It will give us a lot more details than than we previously knew about. We can also see that there's a few more results here that are fake. If we go back to the original image, it says PBS.org season 2018. And if we click on the link here, we also get Alexandria Ocasio-Cortez's full interview on PBS. So Weverify can be just as handy for identifying shallowfakes as it is deepfakes.

[00:25:12] Now, moving on to deepfakes, deepfakes are mostly not used for political purposes. We very rarely see deepfakes that are used for political purposes. Instead, they're most frequently used to target women with online harassment or for satire. We've seen a lot of that as well. And that's because they're still fairly difficult to make. But why don't I walk you guys through two very quick examples so that you understand what a deep fake is and what it looks like.

[00:25:43] And if you're interested in seeing the full versions of these, I've provided the url to you below at these examples. So if you need a second, open those up now.

[00:25:59] Alright. So this first this first deepfake, which was created by an environmental party in the Netherlands. It looks pretty bad. You can see Trump's mouth look moving all over the place here. It it really doesn't look all too genuine. So this you can see he turns here and it's just not great. So it's not great work. It's pretty shoddy. So this one, I think, will be pretty quickly able to say that this is a deepfake or send it to an expert for verification that this is a deepfake.

[00:26:37] Now, let's look at the second case where a politician in Gambia was shown and, here we go, and here you can kind of see that something is off, but it's a little bit trickier to look at. So something that stands out to me right away is that there's very little movement in the eyes. There's not a lot of blinking. There's not a lot of upper facial movement. So this, once again, would be enough context clues for us to send this video for a researcher and begin questioning whether it's genuine.

[00:27:22] Alright. And some final notes on the video. Try different approaches to the same problem as always. Think creatively. Look for telling details in faces and the surroundings. Find context through targeted Facebook or Twitter searches like we learned in the previous lessons. And remember, always archive your evidence, save videos in a separate folder on your computer to avoid archiving errors and make sure to archive any images you come across in case they can't deleted. Or you need to use them as evidence later.

[00:27:57] So that was it. Thank you so much for joining me this week. Thank you so much for engaging with these lessons.

[00:28:06] I really hope you got some interesting ideas out of this week's session. And I can't wait to see how how you approach all of these problems. Please participate in the forums to get some creative thinking around searching and verification on social media going.

[00:28:28] Thank you again. And gear up for a week three with my colleague Craig Silverman, who will teach you all about investigating Web sites.