Module 3 Video 2: Whois searches and website archives

[00:00:00] Hi, welcome to our second video here in week 3, we're going to cover whois and also archive analysis for Web sites.

[00:00:08] I've got a little case study here that we're going to do together. OK. So here's a Yahoo! News article that was published in August of 2020. And at the core here is a claim, a claim that the Antifa.com Web site is number one, redirecting to the political campaign Web site of Joe Biden in the US. And number two, that it has a link to Russia. And so we can see here in the article, you know, someone asked at a White House briefing why antifa.com is redirecting to Joe Biden's Web site. And you don't need to know about American politics and we're not going to go down that rabbit hole on it. But it's all that to say as it was seen as newsworthy and all that to say as it was seen as potentially a negative thing for Joe Biden.

[00:00:52] But this claim about it kind of being linked to Russia is the thing that we want to look at. Now the evidence that they cite is that the domain registration information at one point was listing an address, a name, a company in Russia. OK. So let's dig into that more, because there's a lot to learn and it's really applicable to lots of other scenarios.

[00:01:15] All right. So let's do this together. Get ready to get into your Web browser. All right. So heading over here to Chrome, I'm going to put in antifa.com because we want to see if the claim is true, that when you type that in, it goes to Joe Biden's Web site. And sure enough, it does. OK. So that's true. Someone who owns antifa.com Has decided to to redirect it to Joe Biden's Web site. And the key thing here is anybody can direct a Web site they own to any other Web site. That doesn't mean it has any links to Biden and Yahoo! wasn't claiming that.

[00:01:49] But we do want to understand more about this claim, about a Russia link. And I'm going to show you what they saw that made them make that claim. OK. So here we are on DomainBigData.com. That's one of the Web sites that we're going to be using here. I encourage you to load that up right now in your Web browser. And if you put in antifa.com in the search field there. This is what we're going to see. So this is a typical kind of who is record. It's going to tell us that the Web site, this domain was first registered in 2002. It's going to tell us, you know, the registrant information. So in this case, we see someone or an entity named Whois Privacy Services. And low and behold, we see information related to Russia. But here's the thing. That name, Whois Privacy Services, that tells us that the person who bought this domain name actually paid extra money to make sure their information was private.

[00:02:45] So when you see the registrant information for Whois record listing something like Whois Privacy Services or private registration or something, as in this case, that's linked to potentially a lot of domains. That means that it's a privacy service. It's not actually a person. So the link to Russia simply means that someone decided to pay a Russian privacy service to protect their domain information. Their ownership information. That's not a very strong link, is it? And the other thing I want to draw your attention to here is, you know, there's detailed information. If you scroll down a domain, big data. But what it tells us is that the last time this record was updated was 2017. So now we know that in 2017 it showed this Russian private registration information.

[00:03:31] But can we get anything more recent? And the answer is yes. And that's where we go. And we're gonna try out whoisology. So again, I just entered antifa.com in the search field and this is what we get. And the good thing here is that we can see that whoisology has actually been keeping track of antifa.com and its ownership information since April of 2013. And the record we're seeing right now is from September of 2020. So it's more recent. And when we go in, we look at the registering information. It no longer shows the one that we had before. It's got a different privacy service. Who is guard protected. And this number here shows that that that service is listed with more than 5.5 million other domain names. So it's a popular privacy service, more popular than the Russian one. And it's registered in Panama.

[00:04:22] So, again, we still don't know who actually owns the domain, but we know that in 2017 it had a private register in Russia and now it no longer does. So how do you publish an article claiming a link to Russia when we know it doesn't show that Russian info anymore.

[00:04:38] And we can even dove deeper on this? OK, so normally I would have you look up here, get your Wayback Machine plugin. See that that's where it shows up in your Chrome Web browser and that we could save the page for later. Or we can look at a recent version or the first version of this page. But because Antifa.com is currently redirecting the JoeBiden.com, that's not going to work. So instead, we go to Web.archive.org, we put in Antifa.com. And it's going to bring up the records here of all of the times that Web site has been archived.

[00:05:12] Here's the really interesting thing. If we go back to, you know, 2017, when we know that it had Russian registration information, we can see here that these are all blue dots indicating the days when the page was archived. Now let's skip ahead here to 2020. All of a sudden, we see green dots. What a green dots mean. We'll look down here. Green indicates redirects. So we can see that this domain name was not redirecting, it seems, until as early as May 31 of 2020. But it wasn't as of January. So the redirect from antifa.com to Joe Biden is very recent. Had nothing to do in 2017 when it was owned by someone who used a Russian private service. And now that is linked to a private service registered in Panama. All of a sudden that's when it starts redirecting.

[00:06:05] And, you know, just for reference, if we go back to that time frame when it had the Russian private service and we look. So here's a record from February 23 of 2018. We can scroll up here and choose different days in the Wayback Machine. It says this domain is for sale. So at the time that it had this very tenuous link to Russia, somebody was actually trying to sell the domain. And it only started redirecting to Joe Biden in May of 2020. So that's a quick run through of who is and how we can use archives to actually disprove a claim that was published. You can use this to look up any Web site. You can go back in time on archive.org if it's been archived and you'll find it's really, really helpful.

[00:06:47] So that's it for our second video. Let's move on now and show you a cool tool for connecting Web sites together.