Privacy and Security in Online Social Media
Prof. Ponnurangam Kumaraguru ("PK")
Department of Computer Science and Engineering

Week - 6.2
Lecture – 20
eCrime on Online Social Media

Once again welcome back. This is Privacy and Security in Online Social Media, week 6 the second part.

(Refer Slide Time: 00:18)

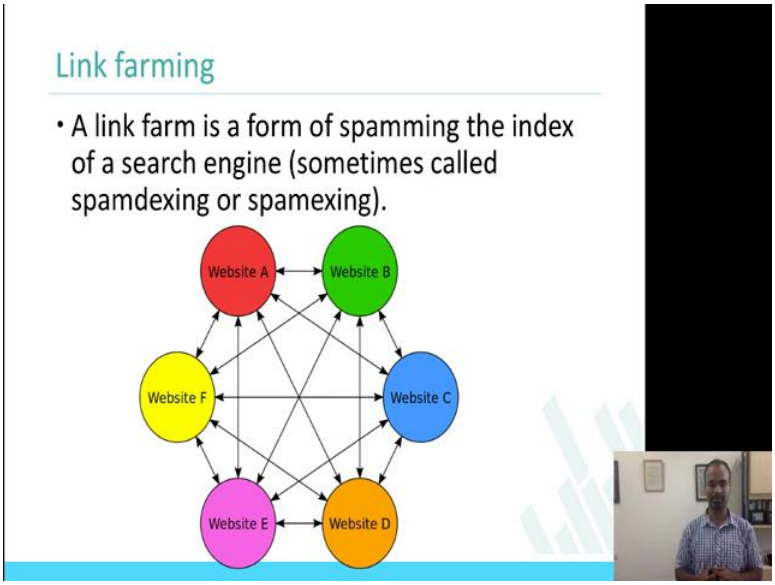
Also in the first part, we generally saw about what e-crimes are, different types of crimes on social networks, specific examples about different crimes; how that affects yor social reputation? How malicious users are actually making use of these social network interactions and topics are answered.

So, what we will see now is some specific problem in social networks, crimes and issues on social networks and we will take some one data set and answer some questions with that data set. Also search engines rank websites basically the Pagerank idea where every page is linked to every page and Pagerank of the rank of every page increases depending on the links that it has with the pages and. So, essentially if you have more of high in-degree helps in increasing the Pagerank.

So, Google works on this technology, where you actually have; you create a website, you link it to, let us take to IIITD's website and IIITD links it back to you, then I think your Pagerank increases heavily, so that is simple idea for Pagerank, but link forming in on the web is basically an idea where websites exchange reciprocal lengths with other sites to improve the rank. So, the idea of making the links between websites which is not otherwise there; creating links or increasing the links of the websites to other websites is actually link farming.

Same ideas are connected to Pagerank. Pagerank is benign or legitimate links that you create. link farming is the idea in which these links are created which are not benign ones.

(Refer Slide Time: 02:12)



So, here is a simple diagram to show that what, how link farming or what link farming is. A link farm is a form of spamming the index of the search engine which is essentially increasing the links between different websites like, for example, website and website A and B. All the, if you start creating links between these websites, if they do not exist and that is called actually link farming. Sometimes, it is also called spamdexing and spamexing. So, that is the idea for link farming. Link farming is a way which non legitimate links are created between the websites. The idea for doing this is when you do this and when you increase the in-degree which is the links that are coming into the website increases then the Pagerank of the website automatically increases.

(Refer Slide Time: 03:04)

So, why link farming in Twitter? So, what we are going to study is, we are going to study the idea of link farming specifically only in the context of Twitter. So, why link farming? What does it help? Who benefits because of actually link farming on Twitter? So, essentially Twitter, I mean given its nature, given amount of data that is getting generated on Twitter, it is basically a web within the web.

If you want to go to, go and look at the out breaking news, Twitter is the place to start with. It has large amount of data on real time news. There is multiple research done to show that Twitter is where news breaks. If you want to look at the latest in now, year 2016, Twitter is probably the best place to look at and people start searching for a topic in Twitter actually meaning Twitter definitely is a micro blogging website, where people push content, but if you look at the pattern in which Twitter is being used, it also being used for search for a topic, live search into people.

So, when you search for a topic in Twitter, the way that the results are presented depends on many factors. So, search engines in Twitter can rank, actually follow ranks. It can actually present the results depending on the connections that you have with the person who is talking about that topic like, for example, if I search for a topic like hash tag year 2016. If any of my friends are talking, it could show up on top. I mean it could show up on the number of followers that people have. If it is a verified account, it should show up on top.

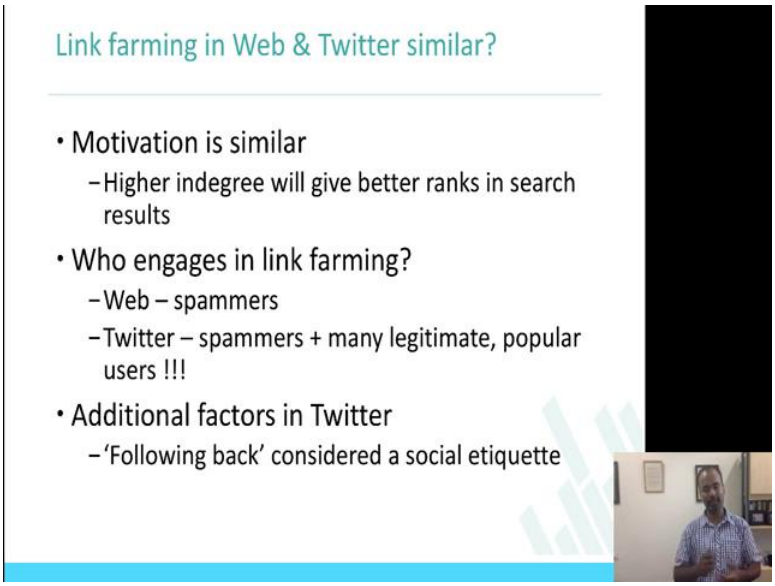
So, the search results can be; search results can be used, these kinds of techniques. PageRank would be one, which is how many people are actually connected to this particular tweet and who are the users, who are connected to this particular tweet. All of this information can be used to actually decide on presenting the search results. Of course, the way that the search results are presented is actually going to bias the users to go to, if twitter is showing you the results on top 5 there is more likely that you are going to actually go look at those particular tweets.

And of course, high in-degree which I think when mentioned the part Pagerank, I said, high in-degree which has number of followers seen as a matter of influence on. number of followers that you have is a measure of social reputation. I also mentioned this in the last part of the week 6. There is a score called Klout. So, I mean I would recommend again you people look at what Klout score is, Klout score is essentially a way by which Klout collates all your online presence, particularly in the social media, and gives numbers to it. For example, my score would be 24, which basically says that on scale of 1 to 100 what kind of influence are you having on the social media services.

Klout is an interesting mechanism that also, a paper which talks about how Klout actually finds out these values and researchers have used Klout score as a way to measure the influence of the users also. Of course, the topic of influencer by itself is actually hard because you are defining who an influencer is; it is becoming more and more difficult. So, while link farming in twitter is basically a large amount of data is getting generated, real time information is spread there and when users search for topic, the information is actually presented depending on the links, depending on the Pagerank, depending on the links that follow a rank depending on the links that users are.

And particularly link farming in Twitter is basically, spammers follow other users and attempt to get them to follow back also. Essentially, how do they increase the in-degree, the in-degree is increased if I am a spammer, I start following thousands and thousands of people and there is a probability that you will actually; the people that I am trying to follow, now will actually follow me back. And again, there is multiple researchers, people who have shown, how the reciprocity can be, there is a high probability that if I follow you, you will follow me back and, giving, with that effect, the link farming actually increases on increases and therefore, twitter can be used to increase the link farm.

(Refer Slide Time: 07:47)

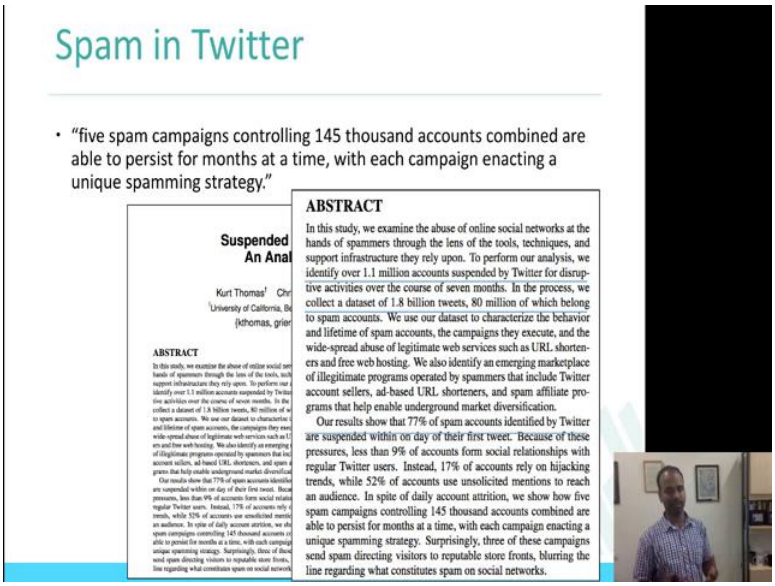


So, here is a slide to show the differences and similarities of link farming in web and Twitter. In the web increasing my Pagerank, increasing my in-degree, increases my probability of showing up in the search results. In the Twitter space, increasing the in-degree actually increases the gain; similarly, to show on my tweets on the search results.

In the webs, spammers actually use link farming. In Twitter, spammers do actually link farming, but it is also done by legitimate and popular users, I think that is the whole idea with where you actually increase the in-degree by making your number of followers high and therefore, you can actually your content can actually be presented to a large number large set of users. And of course, in the context of Twitter, in the context of web, it is not necessary that if I link your website you are probably going to link back to my website; hyperlinks are not created in that way.

Whereas in the context of Twitter there is a high probability that, let us take if I am, I actually follow one of the students who are taking this class, there is a high probability that the student is going to follow me back again and the same way if I follow a professor and the professor probably there is a high probability there the professor will follow me back.

(Refer Slide Time: 09:17)



I thought I will walk you through some literature in the context of spam in Twitter, which is in this case I do not know I think I am going to talk about 2 or 3 research results. Just to tell you, the context of where link farming is going to be kept which is spam in a broader sense. So spam campaigns, here is a paper which is titles 'Suspended Accounts in Retrospect: An analysis of Twitter Spam'. So, 5 spam campaigns controlling 145 thousand accounts combined are able to persist for months at a time. So, here is a zoomed in version of the abstract which reads as, we identify about 1.1 million accounts suspended by Twitter for disruptive activities over the course of 7 months. In the process, we collect a dataset of 1.8 billion tweets and 80 million of which belongs to spam accounts.

The problem with that comes with the spam is that it is not only high in these social networks, but there are actually they also stay for longer. So, here it is 7 spam campaigns controlling 145000 accounts and they persists for multiple months and the another part of the abstract reads as, our results show that 77 percent of spam accounts identified by Twitter are suspended within a day of their first tweet. So, these are some numbers, some idea to get a sense of what is happening in Twitter in the context of spam.

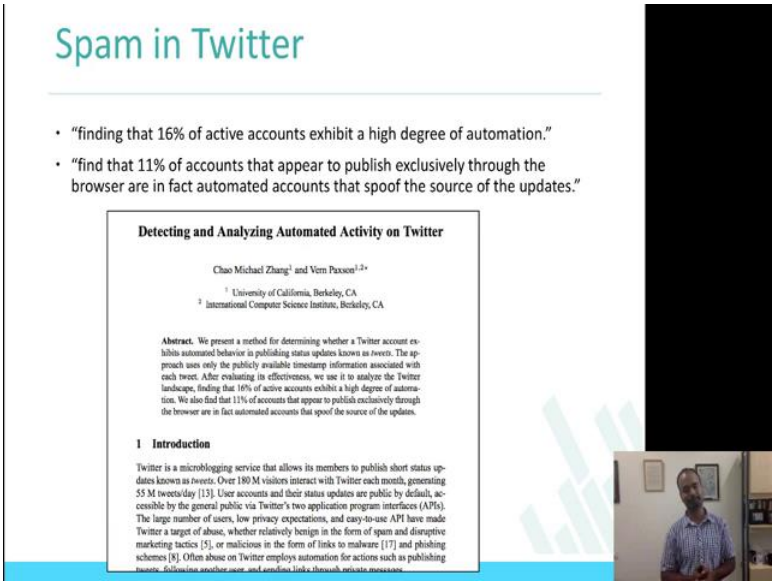
(Refer Slide Time: 10:51)

Here is another one and this paper is also a popular paper in the context of spam on Twitter. So, this is '@spam: The Underground on 140 Characters or Less'. So, what they found is, they found 8 percent of the 25 million URLs posted on the site pointing to phishing, malware and scams. So, that is a lot of URLs which are actually malicious, 8 percent of 25 million URLs, where they are pointing to malware, phishing, scams and malicious ones and they have also found that the click rate is actually higher.

So, they say that, we find that Twitter is a highly successful platform for coercing users to visit spam pages with a click through rate of 0.13 percent compared to, much lower rates previously reported for email spam. So, the idea is that if you get an email of which is which says that please click on this line for buying a product with 10 percent discount that is low probability of you clicking on this link at the email, whereas if the same post is coming from somebody whom you are following on Twitter there is a high probability that you are going to actually check this up. So, that is the probably why this rate is actually high in the context of social networks because it is these posts are coming from your friends.

You remember the Associated Press example that we talked about earlier, where they, where I showed that the post had mentions about White House blast and then they cost actually, why because it is actually coming from Associated Press and there are many people actually follow it and it is also verified account. So, that is why the click rate is

high and as the click rates are higher, it will actually become more and more a successful spam campaign.

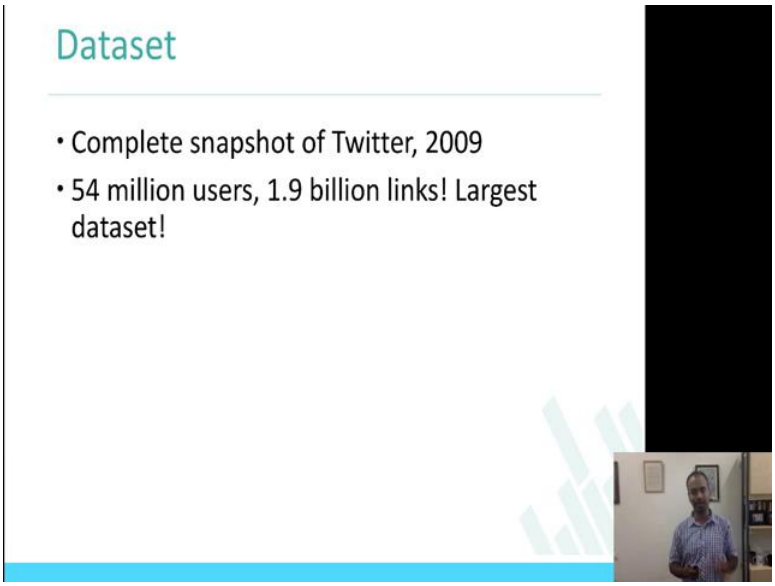


Here is the third one; third research which shows the detecting, which is titled as, 'Detecting and Analyzing Automated Activity on Twitter'. So, what it shows is that 16 percent of active accounts exhibit a high degree of automation. There are again, there are multiple people working on the space in terms of actually identifying automated post on social networks, particularly on Twitter. One simple technique that people try and researchers have tried and it is also being used in some other products is to actually look at the frequency of the post that somebody does, as a human being, you and I probably will not be posting 50 tweets or 45 tweets and, whereas a bot, an automated service would actually do that.

So, people do the graph of hour of the day and minute of the hour; x axis can be the minute of the hour, y axis can be the hour of the day and if you draw the plot, if they are very, very close to each other then there is a high probability that it is actually a automated service that is did this post.

16 percent of the active accounts exhibit a high degree of co-ordination. They also found that the 11 percent of accounts that appear to publish exclusively through the browser are in fact, they are automated accounts that spoof the source of the updates, that is also interesting right. Now, it is not only just the content which is spammed, it is also the spoofing of the source, how the post was done.

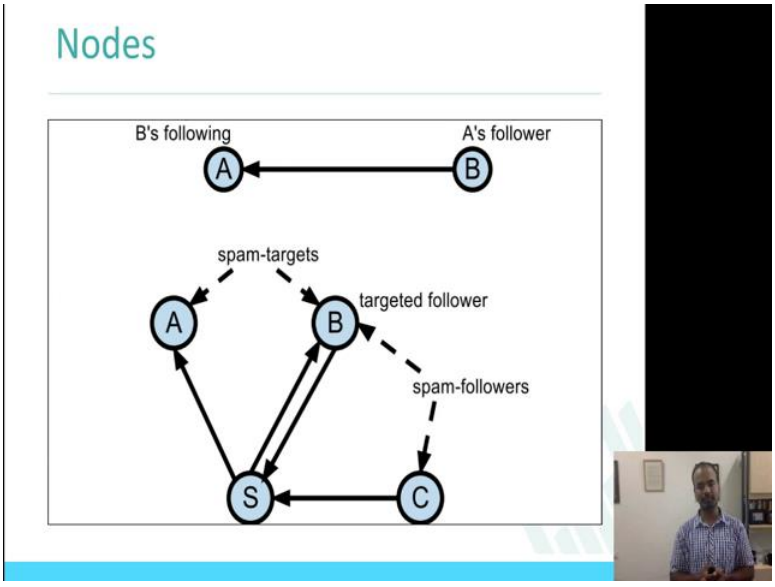
(Refer Slide Time: 14:16)



So, what we are going to look at in the specific questions that we are going to answer is, we are going to actually look at research that was done which is using the entire data set of Twitter, which was collected in 2009. It has 54 million users, I think it will be extremely hard to collect its data today because of the number of users, the connections and probably also the infrastructure that you may need to collect this data.

So, this 2009, 54 million users, 1.9 billion links between the users and it is probably one of the largest set on data largest data set on Twitter.

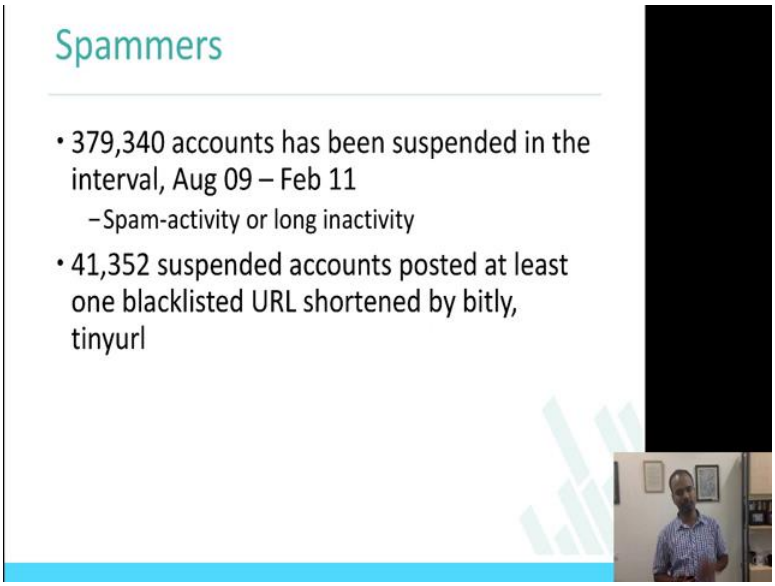
(Refer Slide Time: 14:54)



So, how the definition of the follower and followings is used in this context is, A and B, if there is a link between A and B and going from B to A, they are marked as towards that, then B is, A is B's following and B is A's follower. The error marks towards it which is on the side. So, this is B, which is the follower of A and A is the following of B, I think we talked about what Twitter is, basic terminologies, very early in the course. So, that is follower and following for you. And over the graph at the bottom talks about spam targets which is the targets where spam is going to be sent, targeted follower and spam follower.

So, B and C is basically showing you the spam followers which are which are the ones that are going to be following S, and A and B are the spam targets they are going to be getting the spam from S. So, the terms are going to be follower, following, spam targets where time is going to be spent, sent, spam followers, those are the ones which are going to be following. The base which is B and C or its equivalent to B and first part of the graph spam followers and of course, targeted follower and that makes sense.

(Refer Slide Time: 16:35)

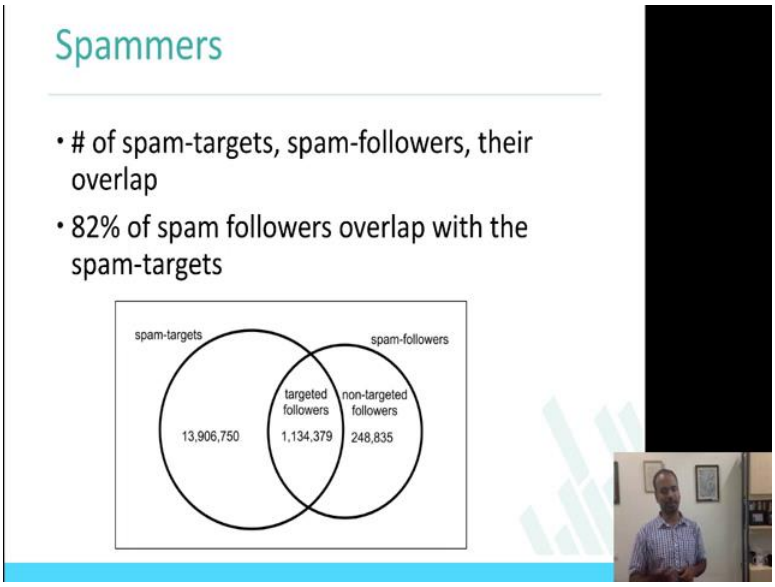


So, what they formed was they formed 379,340 accounts that has been suspended in the interval of this period August 2009 to February 2011, spam activity of course, these accounts were suspended because there was a high spam activity and login activity because if you do not login to your account for sometime, Twitter can actually suspend

your account. 41,352 suspended accounts posted at least one blacklisted URL shortened by bitly or tinyurl. So, there is a set of URL shorteners called bitly, tinyurl.

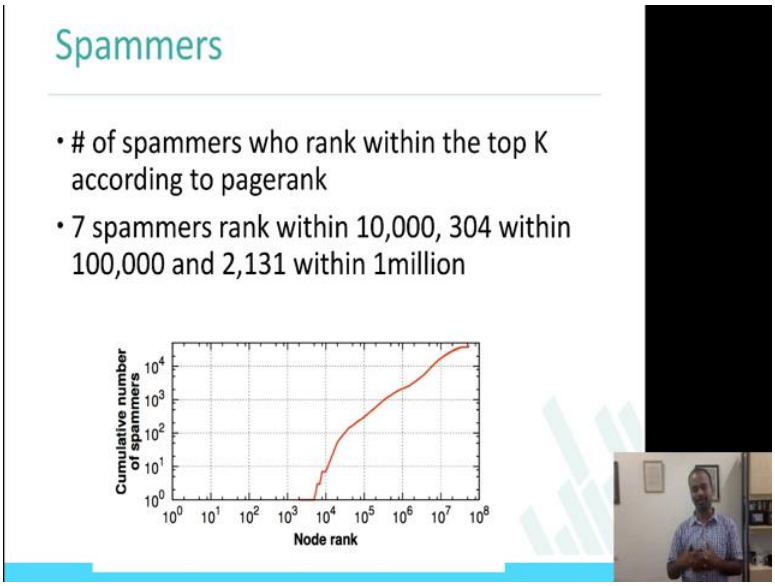
Some of you may have used it, if not please go look at them. The idea for the URL shorteners is, if you want to share a long URL, particularly because of the social networks' influence, social networks' growth, these kinds of URL shorteners have actually become very, very popular because when I want to do a post in Twitter, which is only 140 characters, I do not want to really spend a lot of a space in just posting the URL, instead I would actually send it to the URL shortener, which will reduce the link, if it was like 100 characters it will just give me into bitly, bitly dot com slash some 6 or 8 unique characters which would redirect me to the actual website. So, 41 thousand suspended accounts posted at least one URL, which was actually shortened.

(Refer Slide Time: 18:02)



Let us look at just the spam. So, if you remember the terminology spam targets, spam followers, entire followers. So, number of spam targets followers that the graph at the bottom, actually the Venn diagram at the bottom shows you spam targets were about 13 million, targeted followers, were about 1 million and the spam followers were about 248 thousand, 82 percent of the spam followers overlap with the spam targets alright, which is the followers, spam followers, who are going to be following some accounts are actually part of the spam targets itself, 82 percent of the spam followers overlap with the spam targets.

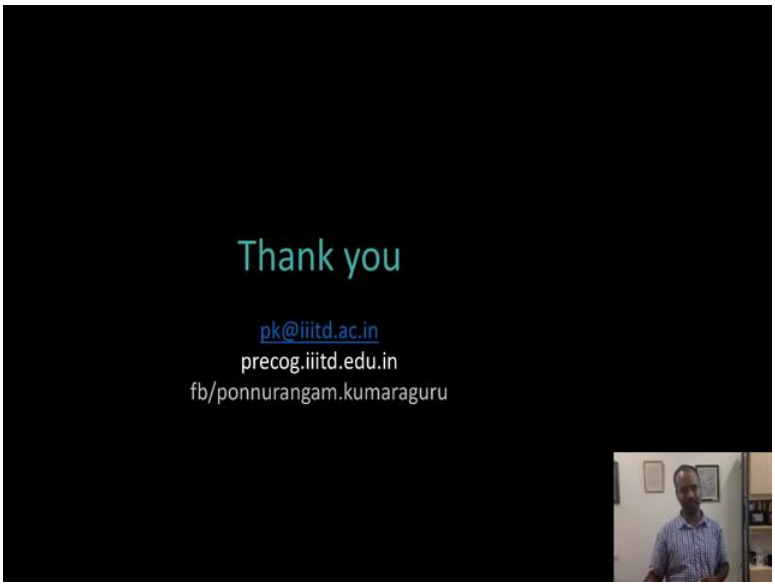
(Refer Slide Time: 18:46)



So, what is the good way? So, here is an interesting way of actually looking at it the data. So, this is cumulative, CDF, which actually shows you node rank at the x axis and cumulative number of spammers in the y axis. There is some interesting conclusions that you can actually draw from this, which is to say that the number of spammers who rank within the top k according to the Pagerank. This is ranked according to the rank of the user. So, if you see within the first 10,000 users there are actually 7 spammers, what does this mean? This means that, if you would actually list down rank of all the users of Twitter, look at the followers, look at the node rank which is the Pagerank, in-degrees of those followers,

you can actually see 7 spammers within the top 10,000 users and 304 within the 100,000 and 2131 within the first 1 million users, which is if you take 10 lakh users, the top 10 lakh users with PageRank, with the in-degree as high, list them, you will see that two thousand users of this 10 lakh users are actually spammers alright. So, that gives you sense of you know the spammers are actually very popular alright. It essentially shows that these users have high in-degree which is the context of the problem that we trying to study which is link farming.

(Refer Slide Time: 20:30)



With that, I will actually stop the second part of the week 6. I will continue with the rest of the results and analysis soon.