

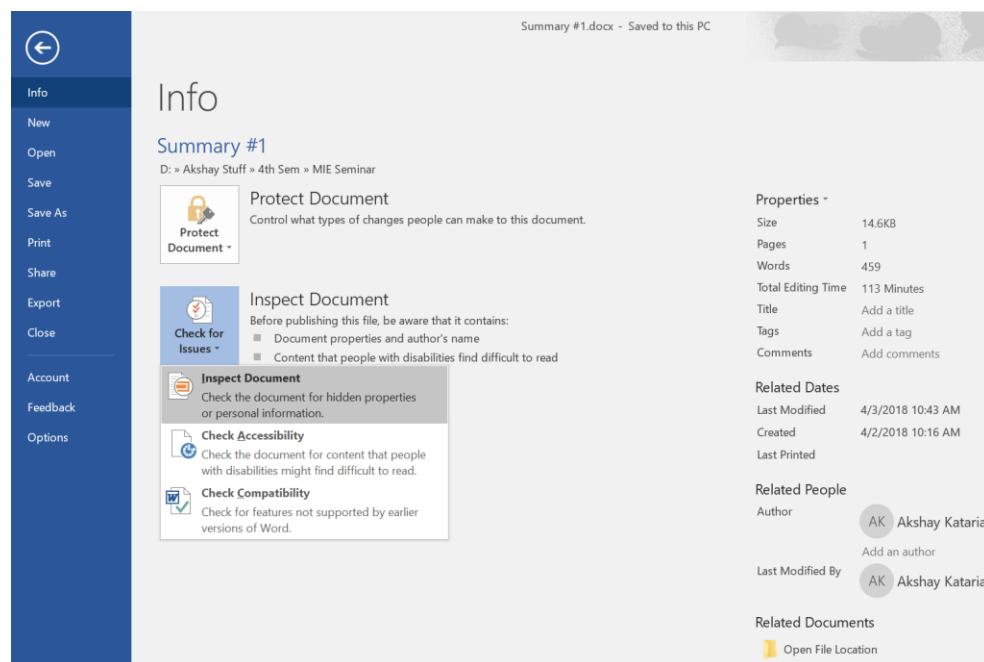
### Ans1. Anonymity in Document Submission

Following are some of the security challenges that are needed to be addressed while submitting the documents online:

- Traceability resistance
- Strong anonymity
- Strong security
- User friendly

Whenever you submit the word or pdf files online, make sure you follow the mentioned steps to remove your personal information before you share it with others.

*For the word documents:*



*Fig1: Snap of the info tab in the word document*

- Information in “Author” and “Last Modified” field along with the other fields can be easily viewed by visiting the info tab inside the word document.
- You can visit “Check for Issues” in the info tab and press “Inspect Document” tab from the drop down menu.
- In the “Inspector Document” dialog box, check all fields and press “remove all”.
- Then press on re-inspect. This will remove all the metadata associated with the word document.
- You also must remove the “Author” and “Last Modified” field.
- This could be done by right clicking the fields and clicking on “Remove Person” tab.

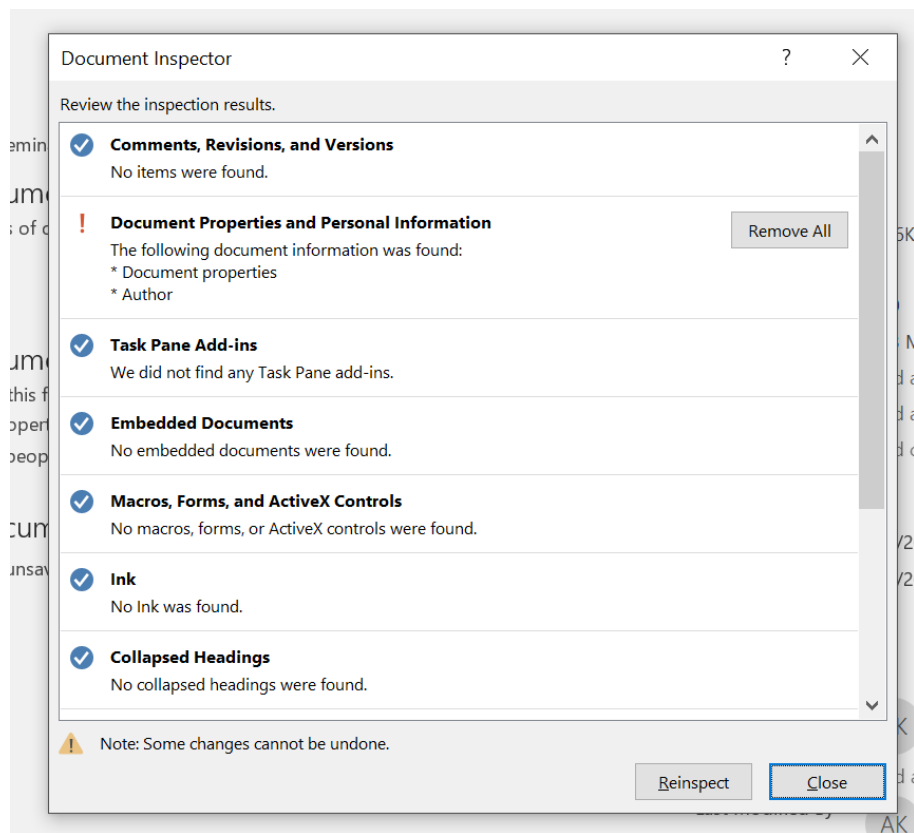


Fig2: Document Inspector dialogue box

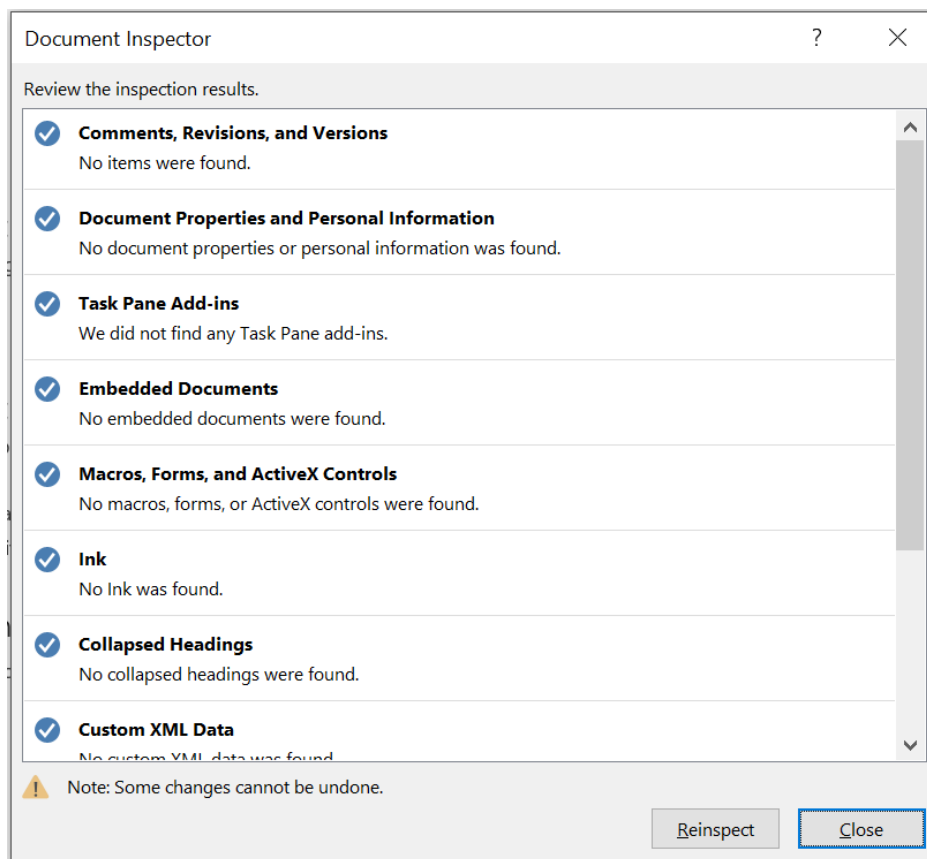
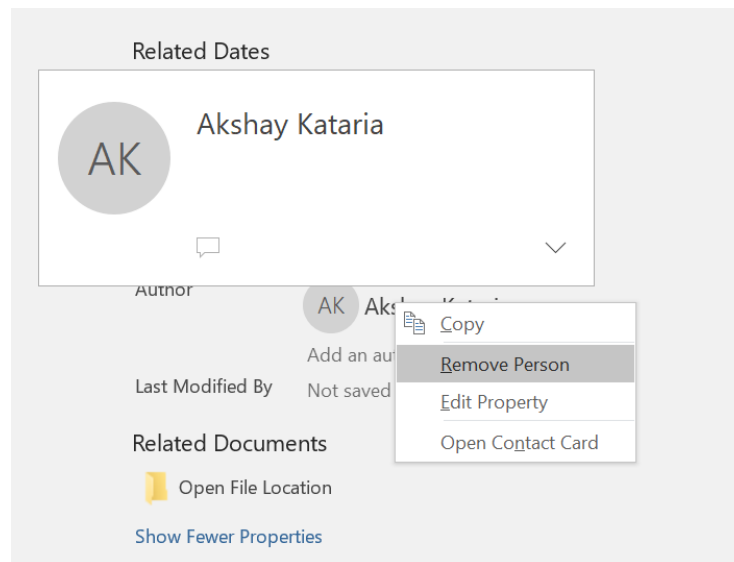
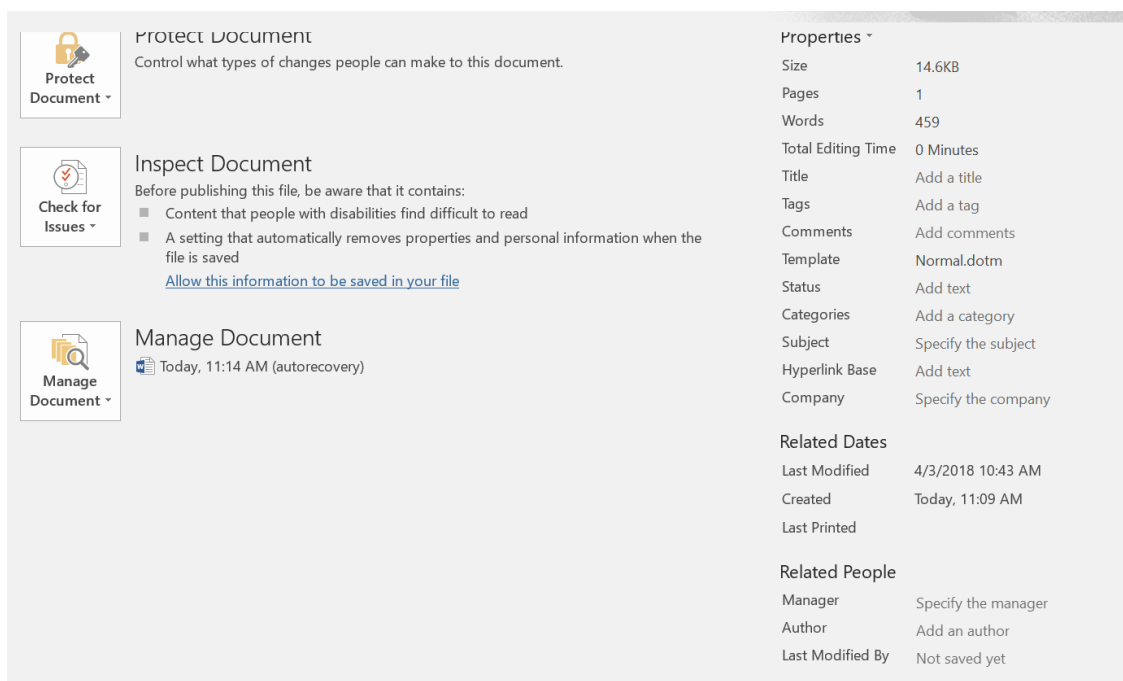


Fig3: Reinspect to make sure metadata has been removed



*Fig4: Removing author from the word document*



*Fig5: No author or Last modified field*

### *For the pdf documents:*

There are few ways through which you can remove all the metadata associated with the pdf files.

- You can first go about removing the comments from the pdf file.
- Click on tools, go to the “Comment” option, select “Show comment list”, select all the comments.
- Then right click on the selected comments, go to Properties and change the name in the Author field from your name to “hidden”.
- Also, you can go to “Tools” in the pdf file and select “Redact” option from that.
- Then choose “Remove Hidden Informaion” button and wait till it completes it processing.
- Then click on “Remove” and Save the file.
- You can also click on “Sanitize Document” under the “Redact” tool itself and can press “Ok” to remove all the metadata associated with your pdf file.

## SUMMARY # 1

Name: Akshay Kataria

UIN: 665336275

Title: Electro-Chemo-Mechanical Degradations and Stabilization in Li-ion Battery Electrodes

Campus Unit: MIE FACULTY CANDIDATE SEMINAR

Date: 03/21/2018

Time: 10:00 am

Speaker

Name: Omer Capraz, PhD

Affiliation: Chemical and Biochemical Engineering, UIUC

The seminar started off with the description about the energy consumption and comparison between the renewable and non-renewable energy. The speaker then described the diverse types of energy storage systems currently in practice, such as: Thermal, Chemical and the Electro-Chemical and then eventually introduced the electro-chemo-mechanical energy systems. All the mentioned energy systems can not perform efficiently till the time they are utilized together. Then the speaker introduced the Li-ion battery and described its properties and needs. He explained the structure of the Li-ion batteries and described the basic properties and operations of the Li-ion batteries. Then the seminar shifted towards discussing the performance degradation of the LMO (Lithium Manganese Oxide) cathodes and how we can customize the cells for stress management with the help of the Electro-Chemo-Mechanical interactions and knowledge of curvature measurement.

The focus then shifted towards customizing the cell for strain measurement and then described the Electro-Chemical cyclic protocol. He then described the process of lithiation and the phase transitions of the of the Lithium Manganese Oxide (LMO). Then moved towards the relation and causes of strain and stress in Lithium Manganese Oxide (LMO) and describing the surface kinetics and the stress generation.

We then discussed the Electrochemical stiffness and the relations that if:

$KE < 0$  then Strain dominates

$KE > 0$  then Stress dominates

The speaker explained the stress and strain derivatives while doing lithiation and eventually explained the stress evolution in Lithium-ion phosphate.

The speaker then described the electrolytes, stating that with the help of 2 electrolytes, 4 different states can be prepared and then supported and elaborated this topic with the help of different graphs and plots.

Fig6: Comments in the pdf file

### SUMMARY # 1

UIN: 665336275

Electro-Chemo-Mechanical Degradations and Stabilization in Li-ion Battery Electrodes

CANDIDATE SEMINAR

Date: 03/21/2018

Time: 10:00 am

Chemical Engineering, UIUC

description about the energy consumption and comparison between the energy. The speaker then described the diverse types of energy storage systems such as: Thermal, Chemical and the Electro-Chemical and then eventually introduced the electro-chemo-mechanical energy systems. All the mentioned energy systems can not perform efficiently until they are utilized together. Then the speaker introduced the Li-ion battery and described its properties and needs. He explained the structure of the Li-ion batteries and described the basic properties and operations of the Li-ion batteries. Then the seminar shifted towards discussing the performance degradation of the LMO (Lithium Manganese Oxide) cathodes and how we can manage with the help of the Electro-Chemo-Mechanical interactions and knowledge of curvature measurement.

customizing the cell for strain measurement and then described the Electro-Chemical cyclic protocol. He then described the process of lithiation and the phase transitions of the Lithium Manganese Oxide (LMO). Then moved towards the relation and causes of strain and stress in Lithium Manganese Oxide (LMO) and describing the surface kinetics and the stress generation.

We then discussed the Electrochemical stiffness and the relations that if:

$KE < 0$  then Strain dominates

$KE > 0$  then Stress dominates

The speaker explained the stress and strain derivatives while doing lithiation and eventually explained the stress evolution in Lithium-ion phosphate.

The speaker then described the electrolytes, stating that with the help of 2 electrolytes, 4 different states can be prepared and then supported and elaborated this topic with the help of different graphs and plots.

The speaker then described the electrolytes on the stress derivatives and investigated the role of the performance in the Li-ion battery and applied the findings while surface

Search Comments...

A Z

Filter

Grid

2 Comments

katar

This is just a test comment !!  
For CS491

Page 1 5/5/2018 11:37 AM

Show Less | Reply

katar

This is Test Comment 2 !  
CS 491

Page 1 5/5/2018 11:37 AM

Show Less | Reply

Fig7: Selecting all the comments from the comment list

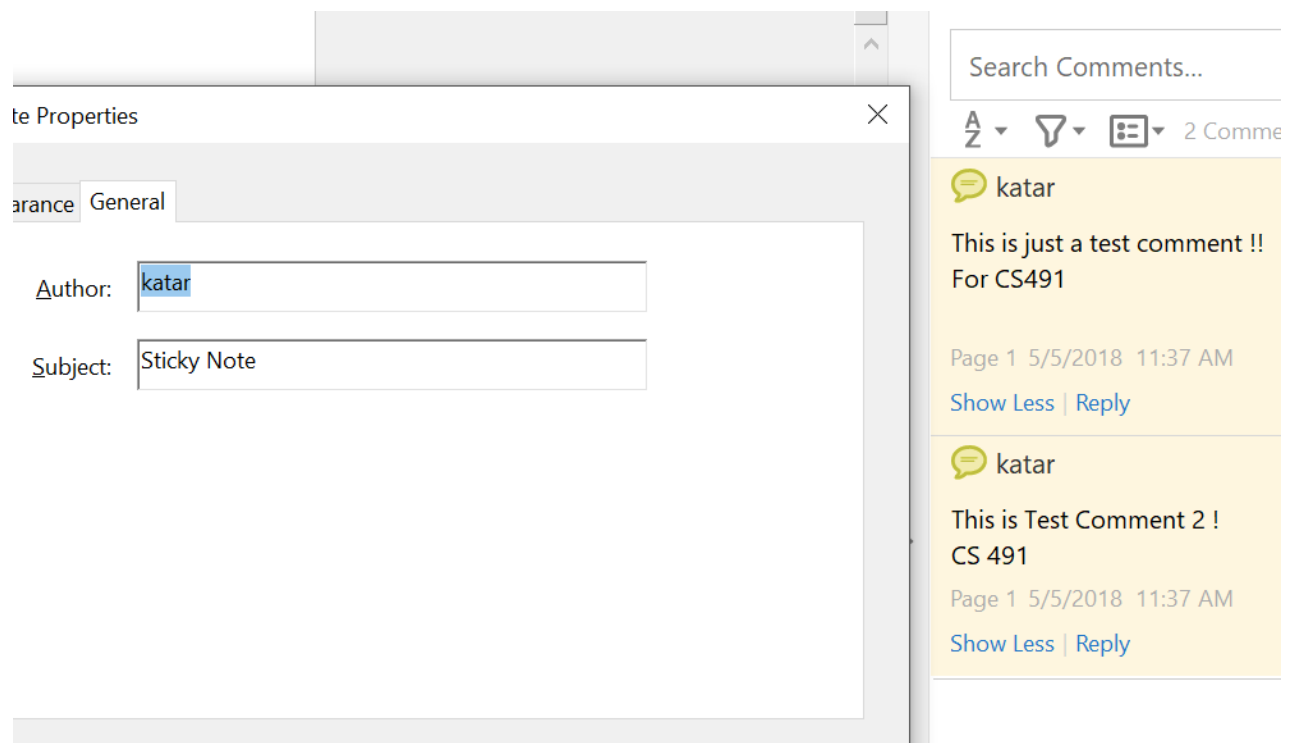


Fig8: Change the name in the author field

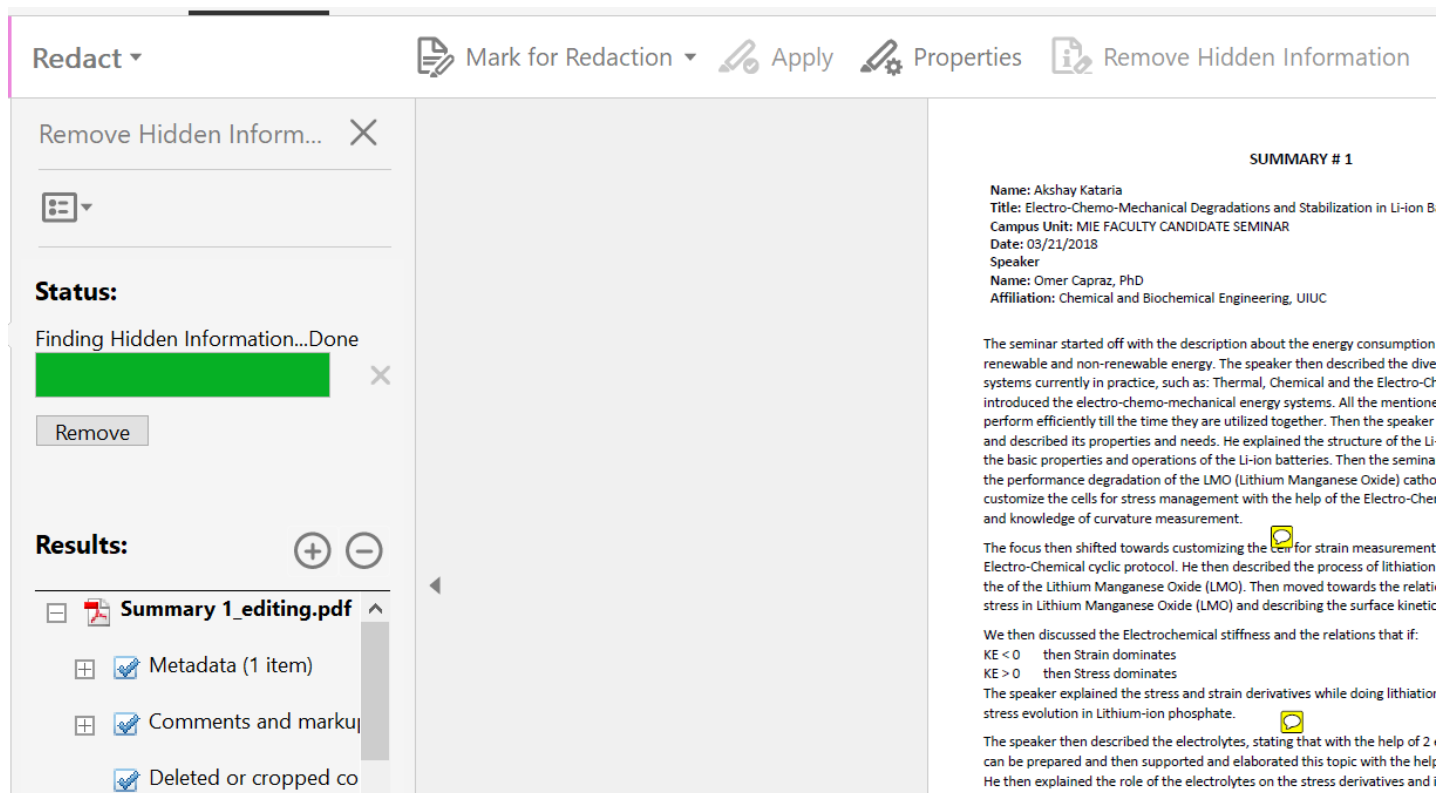


Fig9: Using Redact tool to remove the metadata from the pdf document

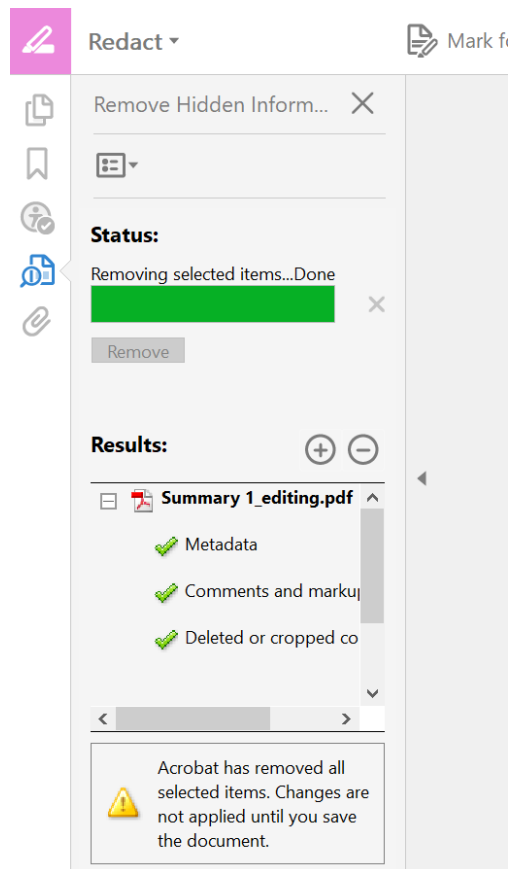


Fig10: Metadata has been removed from the pdf document

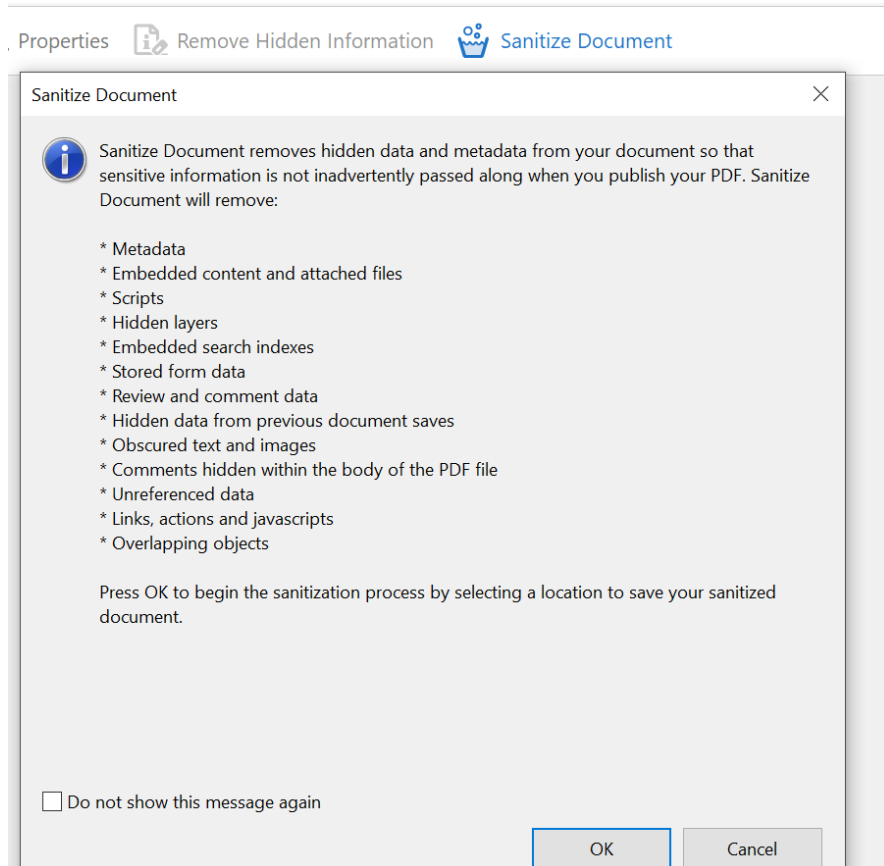


Fig11: Using Sanitize Document under Redact tool to remove the metadata from the pdf document

Any other embedded objects, images or any other kind of object inside your documents can reveal a lot about you. This is known as MetaData. It is the data that describes more about the actual data. It may reveal:

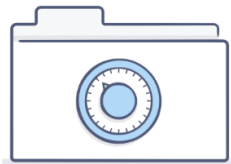
- Date and time the file was created.
- Address or geographical location.
- Type of camera used while taking the image attached to the document and it's settings
- Model or service provider in case you have attached an image taken from your mobile phone.

## Ans2. DropBox

After reading various blogs and exploring security policy of DropBox, I came across various privacy problems that a user can face while storing the data over DropBox. It's scary when you know DropBox holds the master key for every user account and is not afraid to hand it over if some law enforcement needs it. A feature which was also condemned by *Edward Snowden*.

Following are some of the security issues with DropBox:

- Data Retention
- Deleting your account doesn't mean your data have been wiped off
- Your personal info is at risk
- DropBox keeps a track from where you logged in



### How we protect your files

Dropbox is designed with multiple layers of protection across a distributed, reliable infrastructure. Securely access files from desktop, web, and mobile, or through connected third-party apps.



### How we protect your privacy

It's our responsibility to protect your files from unauthorized access. We've designed policies and controls to safeguard the collection, use, and disclosure of your information.



### How to protect your account

Dropbox offers several tools to protect your account from attacks. To help your files safe, enable two-step verification, monitor third-party apps, and adjust your security settings.

Fig12: Features offered by DropBox

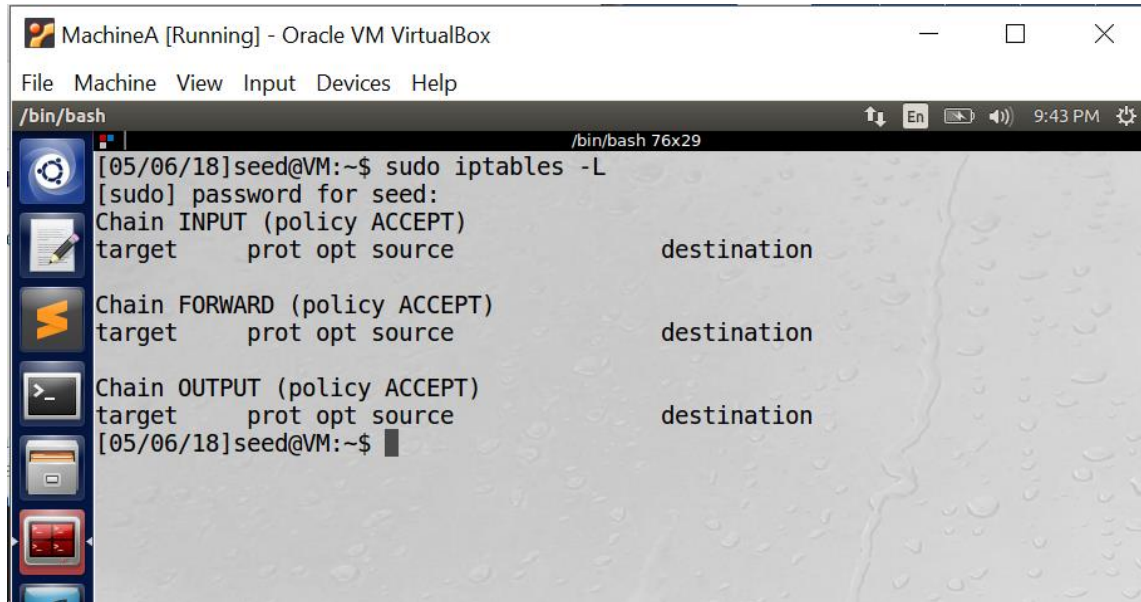
There are few ways in which you can store your data over DropBox more securely which might/might not burden the user. Some of them have been proposed here:

- **Enable Multi Factor Authentication (MFA)**  
Make sure that whenever someone tries to log in to your account, not only they should enter the username, & password but also a code which can be obtained through the apps like the Google Authenticator. This is basically asking for more than one method for authentication which can make your account and the data inside it a bit more secure.
- **Implement Email Notifications**  
Even though it is not a method of making your data more secure on the DropBox platform but definitely this can alert you if your data is being accessed from a different machine.
- **Try to access DropBox via VPN**  
This may again not make your data secure over DropBox but this can definitely help you to avoid the locations from where you might have accessed your account. DropBox won't be able to track your location via your real IP address under the VPN tunnel.
- **Using your own Encryption**  
Try to encrypt your data before it is being uploaded on DropBox. This would definitely be helpful as the company won't have the necessary keys to decrypt your data. Thus making it more secure. Some free encryption softwares are: DiskCrypto, FileVault2, VeraCrypt, etc.



### Ans3. Firewalls

IP tables are by default used as a firewall software in Linux or Unix OS. Syntaxes used to describe the rules are:



```
MachineA [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
/bin/bash
[05/06/18]seed@VM:~$ sudo iptables -L
[sudo] password for seed:
Chain INPUT (policy ACCEPT)
target    prot opt source                destination

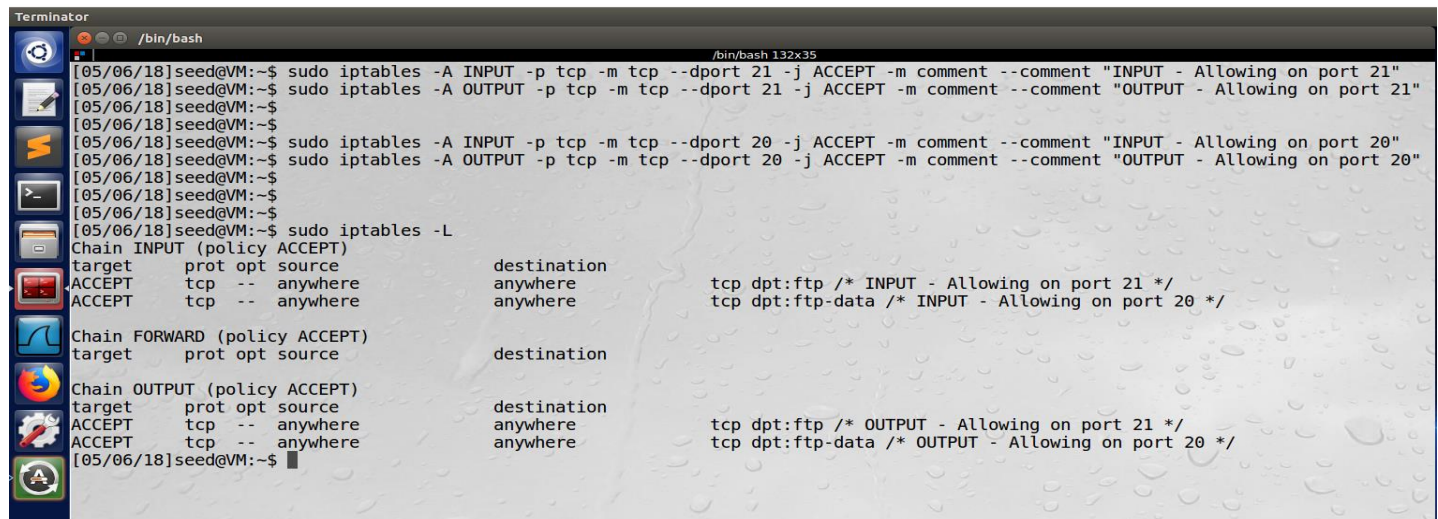
Chain FORWARD (policy ACCEPT)
target    prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target    prot opt source                destination
[05/06/18]seed@VM:~$
```

Fig13: Listing the rules of the IP table firewall

You can list all the current rules in the IP tables with the help of “*sudo iptables -L*”. It requires elevated privileges so it is necessary to use “*sudo*”.

- Allowing FTP traffic



```
Terminator
/bin/bash
[05/06/18]seed@VM:~$ sudo iptables -A INPUT -p tcp -m tcp --dport 21 -j ACCEPT -m comment --comment "INPUT - Allowing on port 21"
[05/06/18]seed@VM:~$ sudo iptables -A OUTPUT -p tcp -m tcp --dport 21 -j ACCEPT -m comment --comment "OUTPUT - Allowing on port 21"
[05/06/18]seed@VM:~$ sudo iptables -A INPUT -p tcp -m tcp --dport 20 -j ACCEPT -m comment --comment "INPUT - Allowing on port 20"
[05/06/18]seed@VM:~$ sudo iptables -A OUTPUT -p tcp -m tcp --dport 20 -j ACCEPT -m comment --comment "OUTPUT - Allowing on port 20"
[05/06/18]seed@VM:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target    prot opt source                destination
ACCEPT    tcp  --  anywhere              anywhere             tcp dpt:ftp /* INPUT - Allowing on port 21 */
ACCEPT    tcp  --  anywhere              anywhere             tcp dpt:ftp-data /* INPUT - Allowing on port 20 */

Chain FORWARD (policy ACCEPT)
target    prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target    prot opt source                destination
ACCEPT    tcp  --  anywhere              anywhere             tcp dpt:ftp /* OUTPUT - Allowing on port 21 */
ACCEPT    tcp  --  anywhere              anywhere             tcp dpt:ftp-data /* OUTPUT - Allowing on port 20 */
[05/06/18]seed@VM:~$
```

Fig14: Entering the rules for allowing the FTP traffic

FTP stands for File Transfer Protocol and there are two ports involved in the FTP protocol (port 20 and port 21). Port #20 is used as a DATA port and Port #21 is used as a Command port at the Server end. Thus both ports are allowed and in both direction. OUTPUT will make sure that the user is able to connect it to host server and INPUT will make sure that the other user is able to connect to the host for file transfers.

- Allowing Mail traffic

SMTP is the industry standard for the mail transmissions i.e. SMTP is used to send and receive the mail messages. This communication takes place at tcp port 25.

```

Terminator
/bin/bash
[05/06/18]seed@VM:~$ sudo iptables -A INPUT -p tcp -m tcp --dport 25 -j ACCEPT -m comment --comment "INPUT - Allowing on port 25"
[05/06/18]seed@VM:~$ sudo iptables -A OUTPUT -p tcp -m tcp --dport 25 -j ACCEPT -m comment --comment "OUTPUT - Allowing on port 25"
[05/06/18]seed@VM:~$
[05/06/18]seed@VM:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
ACCEPT    tcp  --  anywhere              anywhere             tcp dpt:ftp /* INPUT - Allowing on port 21 */
ACCEPT    tcp  --  anywhere              anywhere             tcp dpt:ftp-data /* INPUT - Allowing on port 20 */
ACCEPT    tcp  --  anywhere              anywhere             tcp dpt:smtp /* INPUT - Allowing on port 25 */

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
ACCEPT    tcp  --  anywhere              anywhere             tcp dpt:ftp /* OUTPUT - Allowing on port 21 */
ACCEPT    tcp  --  anywhere              anywhere             tcp dpt:ftp-data /* OUTPUT - Allowing on port 20 */
ACCEPT    tcp  --  anywhere              anywhere             tcp dpt:smtp /* OUTPUT - Allowing on port 25 */
[05/06/18]seed@VM:~$

```

Fig15: Entering the rules for allowing the SMTP traffic

Port #25 is allowed in both the direction. OUTPUT will make sure that the user traffic can reach the SMTP server and INPUT will make sure that the any traffic from within the organization is allowed.

- Reject Telnet traffic

Telnet is used to establish remote connection to your device. By default, this connection is established on TCP port 23. Following is the command through which you can block the Telnet traffic.

```

Terminator
/bin/bash
[05/06/18]seed@VM:~$ sudo iptables -A INPUT -p tcp -m tcp --dport 23 -j REJECT -m comment --comment "INPUT - Rejecting on port 23"
[05/06/18]seed@VM:~$ sudo iptables -A OUTPUT -p tcp -m tcp --dport 23 -j REJECT -m comment --comment "OUTPUT - Rejecting on port 23"
[05/06/18]seed@VM:~$
[05/06/18]seed@VM:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
ACCEPT    tcp  --  anywhere              anywhere             tcp dpt:ftp /* INPUT - Allowing on port 21 */
ACCEPT    tcp  --  anywhere              anywhere             tcp dpt:ftp-data /* INPUT - Allowing on port 20 */
ACCEPT    tcp  --  anywhere              anywhere             tcp dpt:smtp /* INPUT - Allowing on port 25 */
REJECT    tcp  --  anywhere              anywhere             tcp dpt:telnet /* INPUT - Rejecting on port 23 */ reject-with icmp-port-unreachable

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
ACCEPT    tcp  --  anywhere              anywhere             tcp dpt:ftp /* OUTPUT - Allowing on port 21 */
ACCEPT    tcp  --  anywhere              anywhere             tcp dpt:ftp-data /* OUTPUT - Allowing on port 20 */
ACCEPT    tcp  --  anywhere              anywhere             tcp dpt:smtp /* OUTPUT - Allowing on port 25 */
REJECT    tcp  --  anywhere              anywhere             tcp dpt:telnet /* OUTPUT - Rejecting on port 23 */ reject-with icmp-port-unreachable
[05/06/18]seed@VM:~$

```

Fig16: Entering the rules for rejecting the Telnet traffic

#### Ans4. DNS Cache Poisoning

DNS cache poisoning is a cyber attack in which the attacker changes or adds the records in the recursive resolver cache memory so that a DNS query returns the IP address of the attacker's domain instead of the actual one.

a) DNS Cache Attack process is as follows:

- Let's suppose clientA wants to access a particular website, for example "www.why.com".
- As soon as clientA types this name in the web browser, the recursive resolver will first search for this entry in its cache memory.
- If not found, this recursive resolver will visit the local DNS server "cs.uic.edu".
- This DNS server will first check its own cache and if the entry is still not found, it will contact the Root level server.
- This Root level server will direct your DNS server to the TLD's (Top Level Domains) server.
- If your entry is found here, you will get back the IP address. Otherwise, the TLD will again redirect you to the authoritative server.
- From the authoritative server you can get the IP address of the web server where the site is being hosted.
- At this point (at the authoritative server) the attacker will try to pull up the attack and will poison the cache at the authoritative server so it will return the IP address of the attacker.
- In order to return the malicious information, the attacker must know the Transition ID. Once it is known, the attacker's server IP address will be returned by the authoritative server instead of the legitimate one.
- Finding the transition ID would have been an easy task before but now with the version advancements of the software, it is much difficult. Difficult but possible.
- With some time, the transition ID could be figured out. This time can be gained by making the authoritative server a little busy by implementing a DoS attack.
- After obtaining the transition ID, the attacker could send malicious IP address in response to the query generated by the clientA.
- ClientA will use the malicious IP address and this information will be cached inside the local server (cs.uic.edu) and the clientA's device.
- Any device on that local DNS server will now be redirected to the malicious IP if they try to visit "www.why.com".

b) UDP ports are mentioned here as all the DNS queries take place via UDP port unless it's the Zone Transfers. Zone Transfers take place with the help of TCP port.

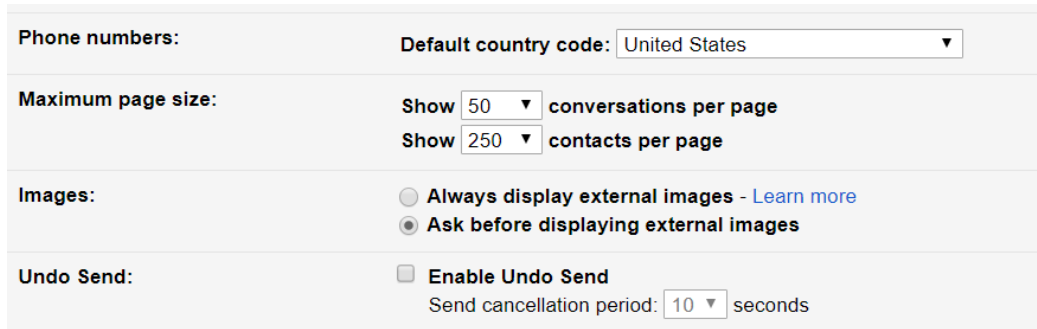
UDP port is 32 bit and transition ID is 16 bit. If we use a brute force attack, it might take around  $2^{48}$  trials.

But there can be other way too.

- Figure out what the destination port can be.
- Then send large number of DNS related queries to the recursive server asking about a random hostname. This is done to make sure that the local server requests the authoritative server.
- Then the attacker can follow each request with a forged reply to anticipate the destination port.

## Ans5. Gmail Image Inlining

Image Inlining with Gmail is switched ON by default but can be turned off by going to the Gmail settings.



The screenshot shows the Gmail settings interface. Under the 'Images' section, the option 'Ask before displaying external images' is selected with a radio button. Other visible settings include 'Phone numbers' with a 'Default country code' dropdown set to 'United States', 'Maximum page size' with 'Show 50 conversations per page' and 'Show 250 contacts per page', and 'Undo Send' with 'Enable Undo Send' checked and a 'Send cancellation period' of 10 seconds.

Fig17: Gmail settings (Automatic Inlining Being Switched Off)

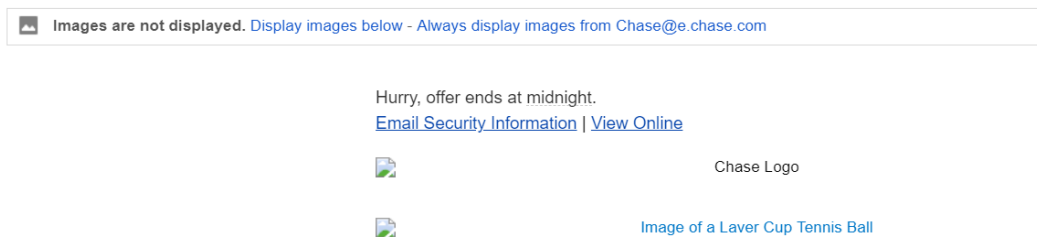


Fig18: Produces a hyperlink for the images to open

Image inlining comes under the CSP (Content Security Policy) standard. This ensures that the content of the emails that you have received shouldn't contain a potential malware like the drive-by-download.

- Images that are sent over the emails could trigger some critical actions where an ordinary GET request can be forged to open up a Spam or Malware URL or could be used as a Phishing attack.
- Also, this could give spammer an idea that your's is a valid and working email address.
- In other cases, by loading these images your email client can give sender the idea that the email has been viewed. This could give information about your browsing activities and the email viewing pattern.

Even after all these vulnerabilities inlining could be turned on in some reasonable options which have been specified below.

- **Trusted Users**  
You can create a whitelist of all the users that are trusted by the client. For this whitelist, you can turn on the inline images.
- **Cache & Load approach**  
The new approach implemented by Google is enhancing the security over emails where instead of allowing the third party to host the images on their own server it is caching the images on Google's server itself. This means that only Google will be able to see your IP address or the device details and not any potential spammer.
- **Alt Text**  
There is an alternate way of conveying your messages. Instead of posting the images inline, we can always go about adding Alternate Text to our images. It is simply the text that is being displayed by the email client instead of the image when the images are being blocked.

### **Ans6. Denial of Service Vs Lack of Capacity**

DDoS attacks basically flood your servers or the routers with the false traffic thereby exploiting the availability of the service to the legitimate users. These days, the attackers ability to masquerade the DDoS traffic as a legitimate one is commendable. It is practically very difficult to distinguish the reasonable traffic with the spoofed one basically because of the ways the DDoS is implemented today.

- Almost all the traffic seems to be coming from a trusted source.
- There are some events (like the one mentioned in the question) that may be an authentic flash crowd.

Following are some proposed methods that may reduce False Positives (denial of services for a legitimate user) and False Negatives (allowing the malicious traffic).

- **Traditional Rate Limitation**  
This solution might work in some cases but the False Positives would be very high. Also, it does not mitigate or identify the attack till the rate of the malicious packets reaches to a particular threshold. Might not be able to detect the attack at all.
- **Check for Referrer field info**  
Referrer is URL data present in the HTTP header field which is used to identify the Web Link from which users are directed to a Web Page. This field can be used in statistical web analysis. Generally, this field would be null in case of targeted DoS attack.
- **Behavioral Analysis**  
We can use AI or other technologies to understand the normal behavior of the application's data flow in order to distinguish between the legitimate and malicious data in the future. A threshold (baseline) behavior can be compared against the spiked traffic and DPI (Deep Packet Inspection) can be used to further analyze the packet if the signatures match.
- **Challenge Response Protocol**  
Most of the DDoS attacks are implemented with the help of the Botnets which are compromised machines that are being controlled via master or attacker itself. If we can send a challenge response mechanism to a suspicious user, we can differentiate between them. A Bot won't be able to solve a mid-level complex problem or a Captcha but a normal user will be able to.
- **Check SNMP (Simple Network Management Protocol)**  
To get an idea if the traffic is due to some misconfiguration or actually because of the DDoS attack, do check the SNMP stats. Also, make sure to monitor the time zones from which the traffic is coming from.