HÖGSKOLAN
DALARNA

Examensarbete

Kandidatexamen

Forensiska Undersökningar av Molntjänster

Cloud Forensics

Författare: Sofia Westberg
Handledare: Hans Jones
Examinator: Pascal Rebreyend
Ämne/huvudområde: Datateknik
Poäng: 15 hp
Betygsdatum: 2012-07-02

Examensarbete nr: E4309D

Högskolan Dalarna
791 88 Falun
Sweden
Tel 023-77 80 00

Förord

Jag vill först och främst tacka min handledare Cecilia Andersson hos PwC som lät mig göra mitt examensarbete hos dem och för den hjälp jag har fått under tiden jag skrivit mitt arbete. Sedan vill jag tacka Martin Lennartsson hos PwC som hjälp mig med arbetet och läst igenom det flera gånger.

Jag vill även tacka alla ni andra som korrekturläst mitt arbete och sett till så att det är förståeligt för de flesta.

Tack!

Sofia Westberg

HÖGSKOLAN DALARNA

EXAMENSARBETE, C-nivå
Datateknik

Program	Reg nr	Omfattning
Digitalbrott & eSäkerhet	E 4309 D	15 p
Namn	Datum	
Sofia Westberg	2012-06-04	
Handledare	Examinator	
Hans Jones	Pascal Rebreyend	
Företag	Kontaktperson vid företag	
PwC	Cecilia Andersson	
Titel		
Forensiska undersökningar av molntjänster		
Nyckelord		
Molntjänst, datormoln, forensik, Office 365, Google Apps		

Sammanfattning

Användning av molntjänster har gjort forensiska undersökningar mer komplicerade. Däremot finns det goda förutsättningar om molnleverantörerna skapar tjänster för att få ut all information. Det skulle göra det enklare och mer tillförlitligt.

Informationen som ska tas ut från molntjänsterna är svår att få ut på ett korrekt sätt. Undersökningen görs inte på en skrivskyddad kopia, utan i en miljö som riskerar att förändras. Det är då möjligt att ändringar görs under tiden datan hämtas ut, vilket inte alltid syns. Det går heller inte att jämföra skillnaderna genom att ta hashsummor på filerna som görs vid forensiska undersökningar av datorer. Därför är det viktigt att dokumentera hur informationen har tagits ut, helst genom att filma datorskärmen under tiden informationen tas ut.

Informationen finns sparad på flera platser då molntjänsterna Office 365 och Google Apps används, både i molnet och på den eller de datorer som har använts för att ansluta till molntjänsten. Webbläsare sparar mycket information om vad som har gjorts. Därför är det viktigt att det går att ta reda på vilka datorer som har använts för att ansluta sig till molntjänsten, vilket idag inte möjligt. Om det är möjligt att undersöka de datorer som använts kan bevis som inte finns kvar i molnet hittas.

Det bästa ur forensisk synvinkel skulle vara om leverantörerna av molntjänster erbjöd en tjänst som hämtar ut all data som rör en användare, inklusive alla relevanta loggar. Då skulle det ske på ett mycket säkrare sätt, då det inte skulle gå att ändra informationen under tiden den hämtas ut.

HÖGSKOLAN DALARNA

DEGREE PROJECT
Computer Engineering

Programme	Reg number	Extent
Digital Forensics and Computer Security	E 4309 D	15 p
Name	Date	
Sofia Westberg	2012-06-04	
Supervisor	Examiner	
Hans Jones	Pascal Rebreyend	
Company	Supervisor at the company	
PwC	Cecilia Andersson	
Title		
Cloud Forensics		
Key words		
Cloud computing, cloud forensics, Office 365, Google Apps		

Abstract

The usage of cloud services has made forensics investigations more complicated. But there are good foundations if the cloud service providers would create services to retrieve all the information. It would make the process easier and more reliable.

The most difficult part to do correctly is to download the information from the cloud services. The investigation is done in a volatile environment and not on a secured copy. It is possible that changes are made during the time the data is retrieved, which is not always visible. It is not possible to compare the differences in files with hash values, in the same way as forensic investigations of computers. That is why it is very important to document how the information is retrieved, preferably by recording the computer screen during the time the information is retrieved.

The information is saved on multiple locations when the cloud services Office 365 and Google Apps are used, both in the cloud and on the computer that is being used to access the cloud. The web browser saves a lot of information of what has been done. That is why it is important to find out which computer has been used to connect to the cloud service, which is not possible today. If it would be possible to examine all the computer that have been used, evidence that is no longer in the cloud could be found,

The best through a forensic angle would be if the cloud service providers offered to retrieve all data which involves a user, including all relevant logs. Then it would be possible to retrieve the data with a secure method, because it would not be possible to change the information during the retrieval.

Innehållsförteckning

1. Introduktion

Idag finns det många program och rutiner för att göra forensiska undersökningar av datorer. När allt fler börjar använda molnbaserade tjänster är det viktigt att det är möjligt att undersöka vad som gjorts genom dessa tjänster. All data sparas inte längre på en dator eller ett företags interna servrar utan fler och fler använder molntjänster för att spara datan externt i molnet.

Det är viktigt att ta reda på hur de forensiska undersökningarna ska göras då molnbaserade tjänster har använts och hur säkert informationen går att få ut utan att integriteten äventyras.

1.1. Bakgrund

Datormoln är en teknik där tjänster erbjuds över Internet. Då behöver inga program installeras på en dator eller server utan allt sköts genom ett webbgränssnitt.

Molntjänster kan till en början delas upp i två modeller, då molnet är privat eller publikt. Ett privat moln är då molnet finns internt hos ett företag, medan ett publikt moln sköts av en annan organisation som tillhandahåller molntjänsterna.

Molntjänster kan sedan delas upp i tre olika modeller av tjänster, se tabell 1.

Molntjänster [1]		
Modell	**Beskrivning**	**Exempel**
Infrastucture as a Service	Infrastrukturen ligger i molnet. Kunden installerar själv ett operativsystem och alla applikationer i molnet.	Amazon Web Services
Platform as a Service	Egna applikationer i molnet, som drivs av en extern leverantör som har infrastrukturen bakom.	Google Apps Engine
Software as a Service	Användning av tjänster som finns i molnet och drivs av en leverantör av molntjänster.	Office 365, Google Apps

Tabell 1 ”Molntjänster”.

En stor fördel och anledningen till att många företag börjar ansluta sig till molntjänster är att det inte behöver installeras något program på en dator och då inte underhållas med uppdateringar. Det blir även billigare eftersom alla kunder delar på samma utrymme hos molnleverantören. De anpassar varje kunds utrymme efter hur mycket som används just vid det tillfället och kan öka eller minska utrymmet så fort det ändras.

Google Apps och Office 365 är exempel av typen ”Software as a Service”, då applikationer som finns i molnet används. Deras tjänster är främst webbaserade kontorsverktyg, där dokument, e-post och annan data finns sparade i molnet istället för på en dator. Office 365 är främst inriktad på att dela dokument mellan användare, medan Google Apps både har dessa möjligheter men också ett väldigt enkelt sätt att ha sina egna dokument i molnet.

1.2. Syfte

Syftet med detta examensarbete är att undersöka hur forensiska undersökningar av molnbaserade tjänster ska utföras framöver samt att undersöka hur tillförlitlig datan är som tas ut. Även vad för typ av data som är möjligt att få ut och var denna data sparas kommer att undersökas.

1.3. Mål

Målet för denna rapport är att ta fram en rutin för hur forensiska undersökningar av molntjänster ska göras på ett korrekt sätt. Både en praktisk och teoretisk rutin ska tas fram för hur det ska göras framöver. För att detta ska vara möjligt är det viktigt att veta hur det ska gå att få ut informationen på ett tillförlitlig sätt.

1.4. Avgränsningar

Rapporten har avgränsats till att undersöka publika molntjänster av typen ”Software as a Service”. Den kommer att inrikta sig på de tekniska aspekterna inom molntjänster och inte ta upp de juridiska problem som kan uppstå. Praktiska forensiska undersökningar kommer att göras på Google Apps och Office 365. Dessa har valts då de är de största leverantörerna av molntjänster som är kontorsverktyg och troligtvis kommer att fortsätta att vara störst närmsta åren.
Den praktiska undersökningen kommer att göras genom en dator med Windows 7. Det kan vara vissa skillnader mellan olika operativsystem och även hur det görs på en mobiltelefon, men detta kommer inte att undersökas i detta examensarbete.

1.5. Frågeställningar

Dessa frågeställningar kommer att undersökas i detta examensarbete.

- Hur ska inhämtning av data ske för att datan ska kunna hämtas på ett sätt att integriteten bevaras?
- Finns det risk att datan som tas ut förändras och inte stämmer överens med vad som har gjorts?
- Är det möjligt att upprepa de forensiska undersökningarna med samma resultat?
- Går det att få ut all data från ett användarkonto?
- Kommer datan att finnas sparad på flera olika platser?
- Går det att tydligt se av vem och när ändringar har gjorts?

2. Utökad bakgrund

Den största skillnaden mellan traditionell kriminalteknik inom IT och för molnbaserade tjänster är var datan finns sparad. Då molntjänster används sparas det mesta av datan externt över Internet istället för på den fysiska datorn som den normalt gör. [2]

Filer som finns på en dator finns kvar tills den skrivs över av ny data och kan alltså återskapas även efter att den har raderats. När en användare raderar ett dokument på sin dator är dokumentet fortfarande kvar, i det oallokerade utrymmet på datorn. Det kan återskapas tills dess att nya filer behöver få plats och då skrivs dokumentet över med de nya filerna. [3]

När program på en dator används sparar de oftast en del användardata direkt på datorn som sedan kan användas som bevis. En dokumenthanterare som Microsoft Word sparar ofta vilka dokument en användare senast har öppnat, allt för att göra det enkelt för en användare att gå tillbaka till tidigare dokument. Denna information kan även vara bra då datorn undersöks forensiskt.

När applikationer över Internet används finns nästan all data i applikationen istället för på datorn. Det betyder att det inte går att leta efter ledtrådar på den fysiska datorn på samma sätt som tidigare.

När en dator undersöks då molntjänster har använts, kommer det mesta av datan inte finnas på lokala datorn, utan sparat hos leverantören av molntjänsten. Den kommer heller inte finnas sparad på en och samma plats. En användare delar utrymme tillsammans med alla andra användare istället för att ha en fysisk del som endast tillhör den användaren. Leverantörer kan även ha datan sparad på flera ställen och då även i flera länder, allt för att upprätthålla säkerheten så att datan inte försvinner eller blir oåtkomligt. [4]

Det konto som finns med an användares filer tar endast upp det utrymme som datan tar, datan flyttas och utrymmet ändrar storlek allt eftersom storleken på datan förändras. Detta görs för att utnyttja allt utrymme på servrarna och inte ta upp onödigt utrymme. Det gör det däremot svårare att få ut en kopia av den del av servern som har använts för en specifik användare eller domän. När filer raderas flyttas datan runt för att fylla igen de tomma utrymmena. På en vanlig dator finns det väldigt mycket information kvar om användaren och gamla raderade filer som fortfarande finns kvar.

Vid forensiska undersökningar av molnbaserade tjänster finns ingen kontroll över vare sig platsen datan finns på eller nätverket runt omkring. Det gör att insamlingen av bevis är ett stort problem för molntjänster. [5]

3. Metod

Den första som kommer att göras är att undersöka hur molntjänster fungerar och vad som hittills har gjorts inom forskning av forensiska undersökningar av molntjänster.

Sedan kommer de två molntjänsterna Office 365 och Google Apps att undersökas. Bakgrundsinformation kommer att sökas på deras hemsidor och deras forum, community.office365.com för Microsoft och groups.google.com för Google.

Praktiska undersökningar ska även göras hos de båda molntjänsterna. Detta syftar till att se hur och om datan förändras och hur forensiska undersökningar ska göras framöver. Både datan som tas ut från molntjänsterna och den data som finns kvar lokalt på datorn ska undersökas i forensiska verktyget EnCase, för att se om något har förändrats. För att kunna göra detta kommer ett företagskonto att skapas med en egen domän, där en administratör har rättigheter har skapa och ändra konton. Det konto som ska undersökas är ett vanligt användarkonto. Information kommer att samlas in både från användarkontot och administratörskontot.

När undersökningen på en dator som använt molntjänsterna ska göras kommer en hårddisk med Windows 7 att användas. Sedan ska e-post, dokument, möten och kontakter skapas i varje webbläsare (Firefox, Chrome & Internet Explorer) för en användare hos varje molntjänst. Varje post som ska skapas kommer att ha ett speciellt ord som sedan kan sökas efter på kopian av hårddisken ska undersökas i EnCase. För dokument kommer både namnet på dokumentet och innehållet att få ett speciellt ord, för e-posten får ämnet och innehållet det. På så vis går dessa ord att sökas efter i EnCase och sedan är det möjligt att se var de finns sparade på datorn någonstans.

Beskrivning för hur all data ska tas fram ur molntjänsterna finns samlat i en guide i bilaga 2, ”Forensiska undersökningar av Office 365 & Google Apps”.

4. Resultat

De forensiska undersökningar som utförs vid användning av molntjänster kan delas in i tre olika delar, som här har delats in i tre olika kapitel, se tabell 2 nedan.

Kapitelindelning		
1	Insamling av data ur molntjänster	Hur datan hämtades ned från molntjänsterna och vad för data som gick att få ut.
2	Forensisk undersökning av nedladdad data ur molntjänster	Hur den nedladdade datan sedan undersöktes och om förändringar i datan hittades.
3	Forensisk undersökning av dator som använt molntjänster	Vad för data som hittades då användarens dator undersöktes.

Tabell 2 ”Kapitelindelning”.

Beskrivningar för exakt hur det ska gå till för att få ut all information på ett korrekt sätt för Office 365 & Google Apps finns i bilaga 2, ”Guide för forensisk undersökning av Office 365 & Google Apps”.

4.1. Insamling av data ur molntjänster

Detta kapitel handlar om vilken information som går att få ut genom att logga in på molntjänsterna, både som administratör och med det användarkonto som undersöks. Hur det ska göras specifikt finns i bilaga 2, ”Guide för forensisk undersökning av Office 365 & Google Apps\Insamling av data ur molntjänst”.

Det finns mycket data lagrad för en användare hos varje molntjänst, däremot är det inte säkert att det är möjligt att få ut all data. Hos tjänsterna Google Apps och Office 365 går det att få ut alla sina filer men metadatan är svårare att få ut. Det kommer alltid att finnas loggar etc. som inte går att få tag på även om de finns. Främst loggar som molnleverantörerna använder för internt bruk. Troligtvis så sparas information om exempelvis från vilken dator och plats en användare anslöt till en molntjänst, som IP-adress, MAC-adress, operativsystem och webbläsare.

När data hämtas ut från en molntjänst är det viktigt att integriteten samtidigt bevaras. Ingen ska i efterhand kunna ifrågasätta resultaten utan det ska tydligt framgå hur datan togs ut och om några förändringar gjordes.

Det är då även viktigt att nedladdningen sker genom en säker anslutning för att inte datan ska gå att modifieras av någon utomstående. All trafik hos Google Apps sker genom HTTPS och blir då krypterad. Hos Office 365 sker all trafik förutom den från Gruppwebbplats genom HTTPS. I Gruppwebbplats finns dokument och den trafiken sker genom HTTP och krypteras alltså inte.

I Google Apps & Office 365 går det att blockera ett användarkonto. Däremot går det inte att få ut någon information utan hela användarkontot blir låst. Detta kan göras medan det bestäms om en forensisk undersökning ska göras. När det väl är bestämt att en forensisk undersökning ska göras måste kontot aktiveras igen och användaren måste låsas ute genom att byta lösenord på användarkontot. På så sätt kommer inte användaren in på kontot men informationen kan fortfarande hämtas ut.

För att visa tydligt att datan endast tas ut och ingen ändrar något kan datorskärmen

filmas då detta görs. [6] Idag finns det många programvaror att använda för att filma datorskärmen, antingen ett specifikt program, exempelvis webbläsaren, eller hela datorns skärm. [7] Det går att filma direkt från att kontot låses upp och lösenordet ändras, under tiden all information tas ut och till dess att kontot låses igen.

I Google Apps är det möjligt att tydligt se när en användares konto blockerats och aktiverats. [8] Det går då att jämföra tiden med filmen för att styrka detta. Detta går däremot inte att göra i Office 365. [9]

Loggar som gäller inloggning kommer att ändras då inloggning görs på användarkontot för att hämta ut datan. Den informationen går endast att få ut en gång och måste därför hämtas först från administratörskontot innan inloggning sker på användarkontot. Denna del kan alltså inte upprepas vid ett senare tillfälle och få ut samma information.

Datan från dokument, e-post etc. går däremot att hämta ut flera gånger och kommer att se likadan ut. I de tester som utförts har inga skillnader upptäckts mellan datan i molntjänsten och efter den tagits ut, se kapitel 4.1.2 – 4.1.4.

4.1.1. Loggar & Statistik

Beroende på vilken molntjänst som har använts går det att få ut olika mängder av statistik i form av loggar. I tabell 3 nedan visas några av de loggar som går att få ut från Office 365 och Google Apps.

Användarspecifika loggar	**Office 365**	**Google Apps [10]**
Senast inloggning (Alla tjänster)	Nej [11]	Ja
Senast inloggning – E-post, kalender, kontakter	Ja, Outlook [12]	Nej
Användarkonto skapat	Nej [13]	Ja
Användarkonto aktiverat	Nej [14]	Ja
Användarkonto låst/blockerat	Nej [15]	Ja
Användarkonto raderat	Nej [16]	Ja
Lösenord ändrat	Nej [17]	Ja

Tabell 3 ”Användarspecifika loggar”.

Microsoft har inga loggar specifika för Office 365 just nu. De loggar som går att få gäller istället andra tjänster från Microsoft som Outlook, SharePoint Server och Exchange Online. [18, 19] Beroende på hur Office 365 används kan dessa loggar vara intressanta, då de ibland samverkar med Office 365. Det är på detta sätt som det går att få ut information om när en användare senast loggade in på e-posten i Office 365. Det är nämligen Outlook som används då. Om en användare loggar in på Office 365 och går direkt in i ”Gruppwebbplats” där dokument finns kommer inte ”Senast inloggning” att uppdateras. Däremot uppdateras det när användaren går in i ”Outlook” för att exempelvis läsa e-post eller lägga upp ett möte.

Google Apps har däremot fler loggar gällande användarkonton. Däremot går det inte att se vilken tjänst en användare loggat in på. Det går endast att se att en användare har loggat in på någon av tjänsterna.

4.1.2. Tidszoner

Det är viktigt att veta vilken tidszon tjänsten är inställd på. Annars kan det bli problem med datum och klockslag när filerna undersöks i ett forensiskt verktyg. Ibland räcker det med att undersöka detta på administratörskontot, men den specifika tjänsten behöver undersökas för att vara säker.

Först och främst går det att se vilken tidszon som gäller för hela domänen på administratörskontot, men många molntjänster låter användaren välja tidszon själv i en eller flera av de olika tjänsterna. Därför måste även tidszonen som är inställd på användarkontot för varje tjänst noteras. [20]

I tabell 4 nedan visas hur Office 365 och Google Apps hanterar ändringar i dokument i olika tidszoner då dokumenten befinner sig i molntjänsten. Dessa tester gjordes ett flertal gånger för varje molntjänst och den tidpunkt som sedan stod registrerades.

Dokument skapat: Tidpunkten som dokumentet skapades och den tidszon som var inställd på tjänsten då detta gjordes.
Dokument ändrat: Tidpunkten som dokumentet ändrades och den tidszon som var inställd på tjänsten då detta gjordes.

Datumstämpel:
Skapat: Tidpunkten som syns i historiken som visar då dokumentet skapades och den tidszon som var inställd på tjänsten då historiken undersöktes.
Ändrat: Tidpunkten som syns i historiken som visar då dokumentet ändrades och den tidszon som var inställd på tjänsten då historiken undersöktes.

Tidszoner	**Office 365**		**Google Apps**	
	Tidszon	Klockslag	Tidszon	Klockslag
Dokument skapas	GMT+1	12:00	GMT+1	12:00
Dokument ändras	GMT+3	14:30	GMT+3	14:30
Datumstämpel:				
Skapat	GMT+1	12:00	GMT+1	12:00 / 14:00 *
Ändrat	GMT+1	12:30	GMT+1	12:30 / 14:30 *

Tabell 4 ”Tidszoner”.

Ovan tester gjordes vid flera tillfällen och för flera olika dokument för att se om det blev någon skillnad i resultatet, men det var ingen skillnad som noterades på grund att detta. I Office 365 gick det inte att se i vilken tidszon en ändring gjorts, utan endast vilken tid ändringen skedde i den egna tidszonen. Det var samma oavsett vilken tidpunkt testet gjordes.

* När tester för detta gjordes i Google Apps stämde inte alltid tiderna. Ibland stod det i historiken i Google Docs att dokumentet skapade 12:00, medan det ibland stod 14:00. Då tidszonen för tjänsten uppdaterades gick det inte igenom fullt på alla platser, vilket gjorde att tiden kunde vara felaktig. Det gick inte att se vilken tidszon som gällde utan endast tidpunkten. Ca 60 % av tillfällena var det 12:00 och 12:30 som angavs, medan resterande tillfällen var det 14:00 och 14:30 som angavs i molntjänsten.

4.1.3. Dokument

Alla dokument som inte var raderade gick enkelt att ta ut ur de båda tjänsterna. Även då försöken upprepades så gick det att få ut samma dokument och inga skillnader upptäcktes. I Google Apps behöver det inte göras genom att gå in i tjänsten för dokument, utan det räcker med att göra det från Google Takeout. Vilket betyder att det inte finns någon möjlighet att ändra i dokumenten då de tas ut. För raderade dokument se kapitel 4.1.3.3.

Google Apps sparar dokument utan filändelser i deras molntjänst Google Docs. För att ta ut ett dokument ur Google Apps måste det först få en filändelse, exempelvis .doc eller .odt. Innehållet i dokumentet kommer inte att förändras och inte heller formen på texten (teckensnitt, storlek etc.).

Kapitel 4.1.3.1 – 4.1.3.3 nedan handlar om den information som går att få ut som rör dokument och vad för problem som uppstod.

4.1.3.1. Datumstämplar

Det är inte möjligt att få fram lika många datumstämplar för dokument i molntjänsterna som med dokument på en dator. I tabell 5 nedan går det att se vilka datumstämplar går att få fram direkt ur molntjänsten genom att logga in på användarkontot. I de filer som sparas på en dator går det att få fram alla de fyra datumstämplarna.

Dokuments datumstämplar i molntjänsten	**Office 365** [21]	**Google Apps** [22]
Fil skapad	Ja	Ja
Senast åtkomst	Nej	Nej
Senast skrivet	Ja	Ja
Post modifierad	Nej	Nej

Tabell 5 ”Dokuments datumstämplar i molntjänsten”.

Det går endast att se det datum ett dokument skapade eller då senaste ändringen gjordes när ett dokument undersöks i molntjänsterna.

4.1.3.2. Dokumenthistorik

Då förändringar görs i ett dokument kan historiska ändringarna sparas i både Google Apps och Office 365. Det görs automatiskt i Google Apps medan funktionen behöver vara aktiverad i Office 365.

Dokumenthistoriken i Google Apps är väldigt tydlig, då det går att se vilken användare som ändrat vad och när det har skett. Det går även att få tillbaka gamla versioner av dokument. I ”Omarbetningshistorik” i Google Docs går det att enkelt klicka runt mellan de olika versionerna. De ändringar som gjorts i varje version är markerade i en färg för varje användare. Det som har raderats syns istället som överstruken text. [23] För att ta ut en tidigare version måste den versionen däremot återskapas.

I Office 365 går det att enkelt se av vem och när en version skapades, men för att se vad som skrevs eller togs bort i en version måste den återskapas.

Om det finns tre versioner av ett dokument, 1.0, 2.0 och 3.0 och det är 2.0 som ska undersökas behöver den versionen återskapas. Version 2.0 blir då även 4.0. Däremot är det möjligt att gå tillbaka till den ursprungliga versionen, 3.0. Detta gör att det är mycket komplicerat att jämföra olika versioner eller ta ut alla versionerna. [24]

Det är även möjligt för en användare i Office 365 att radera tidigare versioner av ett dokument. Då raderas dock alla tidigare versioner, det går inte att välja vilken version som ska raderas. Om detta har gjorts syns det att den första versionen saknas (0.1 eller 1.0). I Google Apps går det inte att radera versionshistoriken, utan enda sättet en användare kan ta bort den är genom att kopiera all text till ett nytt dokument och sedan radera det första dokumentet.

4.1.3.3. Raderade dokument

I tabell 6 går det att se om det går att få tillbaka raderade dokument eller inte från de två olika molntjänsterna.

Raderade dokument	**Office 365** [25]	**Google Apps** [26]
Papperskorgen	Ja, max 30 dagar	Ja
Raderat från papperskorgen	Ja, max 30 dagar	Nej

Tabell 6 ”Raderade dokument”.

I båda tjänsterna hamnar raderade dokument först i en papperskorg där de enkelt kan återskapas eller hämtas ut. Tas det bort från papperskorgen går det i Google Apps inte att återskapa dokumentet, medan i Office 365 hamnar då dokumenten i en administratörspapperskorg. I Office 365 finns dokumenten högst i 30 dagar totalt för de båda papperskorgarna. Alla dokument som en användare har behörighet till kommer att finnas i användarens papperskorg om de har raderats, oavsett vem som raderat dokumentet. Det går endast att se vem som raderat ett dokument i administratörspapperskorgen. Det går även att se vilket datum dokumentet raderades. [27]

För raderade dokument i Office 365 behövde dokumenten återställas till biblioteket med resterande dokument för att de skulle vara möjliga att få ut från molntjänsten. I Google Apps gick det istället att ta ut de direkt ur papperskorgen.

4.1.4. E-post, kalender & kontakter

Det var inga problem då denna information togs ut genom en e-postklient. De e-postmeddelanden som var olästa låg kvar som olästa i e-postklienten och även e-postmeddelanden som fanns i utkast och papperskorgen kom med.

Eftersom ett e-postmeddelande för varje folder (inkorgen, utkast etc.) hade skapats så gick det att se att dessa fanns med i e-postklienten, med samma text som innan. Alltså hade alla e-postmeddelande kommit med. Det blev även samma resultat då detta gjordes om, inget förändrades efter första gången filerna togs ut.

4.2. Forensisk undersökning av nedladdad data från molntjänster

Efter att datan hade hämtats ut ur molntjänsterna undersöktes den i EnCase för att se om förändringar skett med datan. Detta kapitel handlar om vad som gick att få fram ur datan då den undersöktes och vad för förändringar som identifierades.

4.2.1. Dokument

Innehållet i de dokument som togs ut ur molntjänsterna har inte förändrats då dessa

tester har gjorts. Dokument har sett likadana ut som de gjorde i molntjänsterna, både texternas innehåll och formatet. Det går inte att visa att innehållet inte har förändrats genom att ta hashsummor på filerna eftersom andra delar av dokumenten har förändrats då de tagits ut. Dokumentens innehåll har jämförts med verktyg som jämför texter. [28] Då har texten från molntjänsten och texten från det dokument som tagits ut, kopierats och lagts in i verktyget som sedan har jämfört texterna. Inga skillnader i ord eller meningar har då upptäckts. Däremot var det olika mängd mellanslag eller nya rader mellan texterna. Olika ordbehandlingsprogram kan hantera nya rader på olika sätt, vilket gör att det ser ut på olika sätt då de tas in i ett jämförelseprogram. Men det viktigaste, orden, har inte förändras.

4.2.1.1. Datumstämplar

Då forensiska undersökningar av datorer görs har det gått att använda datumstämplar för att se då dokumentet skapades och när en användare senast ändrade i dokumentet. När ett dokument tas ut ur molntjänster kommer inte alla datumstämplarna att stämma. Detta beror på att då dokumenten togs ut skapades de på nytt. De finns inte sparade på samma sätt i molnet som dokument på en dator lagras. När ett dokument tas ut måste filen göras om till den filtyp dokumentet ska vara.

I tabell 7 visas vilka datumstämplar som gick att få ut från de dokument som tagits ut från molntjänsterna. Vid ”Ja” visas den exakta tidpunkten som det skedde i molntjänsten och vid ”Nej” visas istället tidpunkten då dokumentet laddades ned från molntjänsten.

Dokuments datumstämplar i EnCase	**Office 365**	**Google Apps**
Fil skapad	Nej	Nej
Senast åtkomst	Nej	Nej
Senast skriven	Ja	Ja
Post modifierad	Nej	Nej

Tabell 7 ”Dokuments datumstämplar i EnCase”.

När dokument tas ut ur Google Apps och Office 365 kommer datumstämplarna att se ut på samma sätt som när ett dokument kopieras. Tiderna för då dokumenten har skapats, senast åtkomst och modifiering kommer att vara då dokumentet hämtades från molntjänsten, vilket är samma förändring som en kopia av ett dokument får. [29] Däremot är tiden för senast skrivet den tid som någon senast gjorde en ändring i dokumenten i molntjänsten.

4.2.1.2. Tidszoner

Tidszoner kan göra att tiden som visas i EnCase inte stämmer överens med den tidpunkt en förändring gjordes. När ett dokument tas ut från Office 365 eller Google Apps går det inte att se i vilken tidszon en förändring skedde. Läggs dokumenten in i EnCase går det att se tidpunkten dokumentet senast ändrades i den tidszon datorn med EnCase har. Däremot går det inte att se vilken tidszon dokumentet egentligen skrevs i vilket betyder att tiderna inte behöver stämma.

Dokumenten skapades först i molntjänsten, sedan ändrades tidszonen för dokumentet och sist ändrades texten i dokumentet. Efter det togs dokumenten ut och lades in i EnCase. I tabell 8 nedan visas hur tiderna ser ut då ett dokument tas ut ur molntjänsterna och läggs in i EnCase.

Dokument skapat: Tidpunkten som dokumentet skapades och den tidszon

som var inställd på tjänsten då det gjordes.

Dokument ändrat: Tidpunkten som dokumentet ändrades och den tidszon som var inställd på tjänsten då det gjordes.

Senast ändrat enligt EnCase: Den tidpunkt som visas i EnCase då dokument senast ändrades och den tidszon datorn var inställd på då det gjordes.

Tidszoner	**Office 365**		**Google Apps**	
	Tidszon	Klockslag	Tidszon	Klockslag
Dokument skapas	GMT+1	12:00	GMT+1	12:00
Dokument ändras	GMT+3	14:30	GMT+3	14:30
Senast ändrat enligt EnCase	GMT+1	12:30	GMT+1	12:30 / 14:30 *

Tabell 8 ”Tidszoner”.

* När tester för detta gjordes i Google Apps stämde inte alltid tiderna. Ibland visades 12:30 i EnCase och ibland stod tiden som 14:30. De gånger tiden stod som 14:30 stod de även fel i Google Apps under historiken. De gånger det stod 14:30 hade inte tidpunkten ändrats i Google Docs ännu, se kapitel 4.1.2 ”Tidszoner” för mer information.

4.2.2. E-post, kalender & kontakter

Det var inga förändringar i datan då denna information tagits ut. Då datan undersöktes i EnCase såg den likadan ut som den gjorde i molntjänsterna. Däremot går det inte att visa genom att ta hashsummor på filerna som när en fil som finns på en dator undersöks. Datan sparas inte på samma sätt då den lagras i molntjänsten som på en dator och kommer då att förändras då den tas ut, även om själva innehållet inte förändras. Det gick istället att se att innehållet var densamma då de e-postmeddelande, möten och kontakter som skapats hade korta namn som sedan letades efter i EnCase.

4.3. Forensisk undersökning av dator som använt molntjänster

Mycket information kan hittas utan att logga in på användarkontot hos molntjänsten då webbläsarna lagrar väldigt mycket data. E-post som har skickats eller öppnats i en webbläsare utan att de har laddats ned till en e-postklient kan ändå finnas sparad på datorn. Den data som går att få ut från datorn kan även innehålla gammal information, beroende på när den senast anslöts till Internet.

Webbläsarna lagrar data från hemsidor som är besökta främst på en plats på datorn. [30] Data som raderats från webbläsarnas cache kan även finnas kvar på datorn i det oallokerade utrymmet. Det är det utrymmet som inte används, där det fortfarande kan finnas information kvar. När en fil raderas blir den plats där datan finns skriven oallokerad, men datan tas inte bort förrän den skrivs över med ny data.

I kapitel 4.3.1 – 4.3.4 nedan går det att se vad för data som hittades genom webbläsarna och även det som hittades i det oallokerade utrymmet. I bilaga 2, ”Guide för forensisk undersökning av Office 365 & Google Apps\Forensisk undersökning av dator som använt molntjänst\Webbläsardata” går det att se var de olika webbläsarna lagrar sin användardata. Informationen lagras på samma plats för de olika typerna av data.

4.3.1. Dokument

I tabell 9 nedan går det att se de dokument som gick att få ut från de tre webbläsarna då den forensiska undersökningen av datorn gjordes. En del data hittades även i oallokerade utrymmen på hårddisken och kan då komma från någon av de tre webbläsarna. I både Office 365 och Google Apps kan användaren läsa dokument utan att en Internetanslutning finns, i Office 365 går det även att redigera dokumenten då. För att det ska fungera används för Office 365 programmet SharePoint Workspace. För Google Apps används webbläsaren Google Chrome, med appen Google Docs. Så fort Internetanslutning finns så synkroniseras dokumenten så att det blir uppdaterat i molnet. [31] I tabell 8 står Google Apps offlinetjänst som ”Chrome Offline”.

Skapat: Skapat ett dokument i den specifika webbläsaren.
Borttaget: Raderat ett dokument i den specifika webbläsaren.
Rubrik: Namn på dokumentet.
Innehåll: Text i dokumentet.
E.T: Ej tillämplig

Dokument	**Office 365**	**Google Apps**
Firefox		
Skapat – Rubrik	Ja	Ja
Skapat – Innehåll	Nej	Nej
Borttaget – Rubrik	Ja	Nej
Borttaget – Innehåll	Nej	Nej
Chrome		
Skapat – Rubrik	Ja	Ja
Skapat – Innehåll	Nej	Nej
Borttaget – Rubrik	Nej	Ja
Borttaget – Innehåll	Nej	Nej
Internet Explorer		
Skapat – Rubrik	Ja	Nej
Skapat – Innehåll	Nej	Nej
Borttaget – Rubrik	Ja	Ja
Borttaget – Innehåll	Nej	Ja
Chrome Offline		
Skapat – Rubrik	E.T	Ja
Skapat – Innehåll	E.T	Ja
Borttaget – Rubrik	E.T	Nej *
Borttaget – Innehåll	E.T	Nej *
Sharepoint Workspace		
Skapat – Rubrik	Ja	E.T
Skapat – Innehåll	Nej	E.T

Borttaget – Rubrik	Nej	E.T
Borttaget – Innehåll	Nej	E.T
Oallokerat utrymme		
Skapat – Rubrik	Ja	Ja
Skapat – Innehåll	Nej	Nej
Borttaget – Rubrik	Ja	Ja
Borttaget – Innehåll	Nej	Nej

Tabell 9 ”Dokument”.

* Raderade dokument från Google Apps kan finnas kvar en stund. Detta uppdateras inte lika fort som ändringar och nya dokument. Men efter ca 10 min tas de raderade dokumentet bort ur databasfilen med alla dokument. Ändringar i dokument uppdateras oftast inom en minut.

Raderade dokument togs bort ur databasfilen oavsett om ändringar hade gjorts i andra dokument, nya dokument hade lagts till eller då inget annat gjorts. De dokument som togs bort skrevs inte bara över av ny data, utan togs helt bort ur filen.

Innehållet från de dokument som sparats ned för offline användning i SharePoint Workspace gick inte att hitta genom en forensisk undersökning av datorn i EnCase. Endast rubrikerna hittades. Dokument lagras i en allmän Office-fil som kallas Office Document Cache (ODC). [32]

Då ett dokument hittades i EnCase från Office 365 och Google Apps så hittades det inte som ett helt dokument där det tydligt syns namnet på dokumentet och innehållet. Rubriker och innehållen hittades många gånger på olika platser och det gick inte alltid att se tydligt att de hörde ihop. Det är alltså mycket tydligare då informationen tas ut direkt från molntjänsten än genom datorn som har använts.

4.3.2. E-post

I tabell 10 nedan visas den e-post som gick att få ut från de tre webbläsarna då den forensiska undersökningen av en dator gjordes. En del data hittades även på oallokerade utrymmen på hårddisken och kan då komma från någon av de tre webbläsarna.

Ämne: E-postens ämnesrad.
Innehåll: E-postens innehåll.
Inkorg: E-post i inkorgen har öppnats i webbläsaren.
Papperskorg: E-post i papperskorg har öppnats i webbläsaren.
Utkast: E-post i utkast har öppnats i webbläsaren.
Skickat: E-post har skickats från webbläsaren.

E-post	**Office 365**	**Google Apps**
Firefox		
Inkorg – Ämne	Nej	Ja
Inkorg – Innehåll	Ja	Ja
Papperskorg – Ämne	Nej	Nej
Papperskorg – Innehåll	Nej	Nej

Utkast – Ämne	Nej	Ja
Utkast – Innehåll	Ja	Ja
Skickat – Ämne	Nej	Ja
Skickat – Innehåll	Ja	Ja
Chrome		
Inkorg – Ämne	Ja	Nej
Inkorg – Innehåll	Ja	Ja
Papperskorg – Ämne	Nej	Nej
Papperskorg – Innehåll	Nej	Nej
Utkast – Ämne	Nej	Nej
Utkast – Innehåll	Ja	Nej
Skickat – Ämne	Ja	Nej
Skickat – Innehåll	Ja	Ja
Internet Explorer		
Inkorg – Ämne	Nej	Nej
Inkorg – Innehåll	Ja	Ja
Papperskorg – Ämne	Nej	Nej
Papperskorg – Innehåll	Nej	Nej
Utkast – Ämne	Nej	Nej
Utkast – Innehåll	Ja	Nej
Skickat – Ämne	Ja	Nej
Skickat – Innehåll	Nej	Nej
Oallokerat utrymme		
Inkorg – Ämne	Nej	Nej
Inkorg – Innehåll	Nej	Ja
Papperskorg – Ämne	Nej	Nej
Papperskorg – Innehåll	Nej	Nej
Utkast – Ämne	Nej	Nej
Utkast – Innehåll	Ja	Nej
Skickat – Ämne	Nej	Nej
Skickat – Innehåll	Ja	Ja

Tabell 10 ”E-post”.

Det e-post som låg i papperskorgen och som öppnades i varje webbläsare fanns inte sparad någonstans på datorn. E-posten i inkorgen, utkast och de som har skickats har hittats i vissa webbläsare och ibland för den ena tjänsten men inte den andra. Ibland har även endast innehållet i ett e-post hittats, medan andra gånger så är det ämnet som hittats.

4.3.3. Kontakter

Kontakter som skapats i en webbläsare hittades inte på den dator som undersöktes, varken för Google Apps eller Office 365. Ingen information om en kontakt som hade lagts till i någon av molntjänsterna genom webbläsarna hittades.

4.3.4. Kalender

I tabell 11 visas de möten som hittades på den dator som undersöktes för respektive webbläsare. Ett möte hade skapats i varje webbläsare för de två molntjänsterna. Mötet hade ett ämne och ett datum. Vid ”Ja” så hittades mötets ämne, vid ”Nej” så hittades ingen information om mötet.

Kalender	**Office 365**	**Google Apps**
Firefox	Ja	Nej
Chrome	Nej	Nej
Internet Explorer	Nej	Nej
Chrome	Nej	Nej
Oallokerat utrymme	Ja	Nej

Tabell 11 ”Kalender”.

Det datum mötet var inlagt på hittades inte i samband med texten för mötet. Inte heller annan information om mötet hittades.

5. Diskussion

När molntjänster används räcker det inte med att ta en kopia av en hårddisk för att få ut all information. Informationen måste hämtas från molntjänsten och den eller de datorer som har använts för att ansluta till molntjänsten. Ett problem då så mycket information som möjligt ska gå att få ut är att det är svårt att veta vilka datorer en användare har använt. Då kan utredaren gå miste om värdefull information.

5.1. Insamling av data ur molntjänster

Att samla in all information som finns hos molntjänsterna är den svåraste delen av den forensiska undersökningen. Det är även den viktigaste delen eftersom nästan all information finns sparad i molntjänsten och inte på den fysiska datorn som har använts.

Det går inte att be leverantören av molntjänsten om en fysisk kopia av allt som rör en domän, då datan inte är tydligt delad mellan olika kunder hos leverantören. Informationen kan finnas spridd mellan flera olika servrar och även i flera olika länder.

All information som ska tas ut måste alltså tas ut genom inloggning på den specifika domänens konto hos molntjänsten. När all information ska samlas in från en molntjänst går det inte att göra det med samma metod som när en kopia av en hårddisk tas. Det går inte att använda skrivskyddad utrustning som ser till att endast en kopia tas. När informationen ska tas ut från en molntjänst över Internet måste förfrågningar skickas till molntjänsten för att det ska gå att få ut informationen.

Eftersom trafiken i Google Apps sker genom HTTPS så blir den trafiken krypterad och är då skyddas datan som skickas från att avlyssnas eller förändras. I Office 365 är endast delar av tjänsten skyddad på detta vis. All trafik som skickas när användaren är inne i Gruppwebbplats sker okrypterat. Vilket betyder att då utredaren ska ta ut den data som finns lagrad där, dokumenten, så kommer de att tas ut genom en osäker anslutning. Detta är något som Office 365 borde ändra på, både för att göra det säkrare för kunderna och då utredningar görs.

Det går i de flesta tjänsterna inte att ta ut informationen utan att göra några ändringar alls. Loggar om exempelvis senaste inloggningen kommer att ändras då utredaren loggar in för att ta ut informationen. Därför är det viktigt att ta ut loggarna först genom administratörskontot, innan inloggning på användarkontot görs.

För att kunna bevisa att inget ändrades i datan då den togs ut är det en bra idé att filma datorskärmen då det görs. Då är det enkelt att gå tillbaka och visa vad som gjordes och att inga förändringar gjordes samtidigt. Det är även bra om det går att visa att kontot har varit låst både innan och efter att det gjordes, vilket går i Google Apps.

För att få ut all information från molntjänsterna Office 365 och Google Apps just nu behöver inloggning ske både på administratörskontot och det användarkonto som undersöks. Informationen behöver även hämtas från flera platser. Skulle det gå att få ut all information genom en tjänst skulle det vara väldigt praktiskt. Det skulle även vara säkrare ur forensisk synvinkel, då utredaren inte skulle vara inne och rota bland dokument och e-post.

Några anställda hos Google har som mål att göra det enklare för användare att få ut sin data ur Googles produkter genom föreningen dataliberation.org. De tycker att det är

viktigt att en användare enkelt ska kunna få ut all sin information och flytta mellan olika företags tjänster. Därifrån kommer tjänsten Google Takeout. Med den tjänsten går det att få ut alla dokument och även data från några andra tjänster enkelt. Om det skulle utvecklas till att gälla även metadata skulle det vara väldigt bra för forensiska undersökningar.

Varken i Office 365 eller Google Apps går det idag att få ut loggar gällande varifrån en användare har anslutit sig till molntjänsterna. IP-adresser, MAC-adresser, operativsystem och webbläsare är information som skulle vara väldigt intressant information då det visar varifrån en användare har anslutit sig och med vilken dator det har skett. Då skulle det gå att se om flera datorer eller mobiltelefoner har använts. Troligtvis loggar många molnleverantörer detta i statistiskt syfte. Exempelvis Google är kända för att samla in mycket information vid användning av deras tjänster. Även loggar om när användare har öppnat dokument är information som skulle vara intressant.

5.1.1. Tidszoner

När dokument som skrivits i olika tidszoner togs ut blev det inte alltid samma resultat för Google Apps. Ibland ställdes inte tidszonen om innan ett dokument togs ut. Efter att det testats ett flertal gånger, verkade det som om tidszonen uppdaterades efter en stund, det skedde inte alltid på en gång. Detta verkade ske då ett dokument togs ut strax efter att tidszonen hade ändrats. Google Docs hann då inte reagera på att användaren var i en annan tidszon än den tidszon som texten skrevs i. Det viktiga är inte att tiden förändras till en annan tidszon utan att den antingen förändras eller inte. Det blir problem när tiden ibland förändras efter tidszonen och ibland inte. Det är viktigt att vara säker på om det har skett.

Allra bäst vore det om det tydligt stod både vilken tidpunkt och i vilken tidszon något gjordes.

5.1.2. Dokument

Molntjänsterna sparar väldigt mycket information om dokumenten, förändringar som gjorts, av vem och när de gjorts osv. Samtidigt är det väldigt svårt att få ut den informationen på ett enkelt sätt, både ur Office 365 och Google Apps. För att se vilka användare ett dokument tillhör måste det specifika dokumentet markeras och sedan måste utredaren gör några klick för att få fram informationen. Den går alltså inte att ladda ned och undersöka senare. För att få fram den informationen för alla dokument måste samma procedur göras för varje dokument. Det är ett väldigt tidskrävande arbete och för att få ut informationen måste datorskärmen filmas under tiden med ett inspelningsverktyg så att den finns kvar. Samma gäller för att se vem som har ändrat ett dokument i Office 365.

När det gäller vad som ändrats i ett dokument går det i Office 365 endast att se det om en tidigare version återskapas. När det görs så ersätter den istället den senaste versionen. Vilket betyder att stora ändringar i dokumentet har gjorts. Det går inte att ta ut en tidigare version utan att ersätta den senaste versionen. När det görs medför det så pass stora förändringar där innehållet i filerna förändras, vilket inte får ske vid en forensisk undersökning.

I Google Apps däremot går det att klicka runt bland de olika versionerna och se ändringarna som har gjorts utan att påverka dokumentet. Då en användare är inne på

historiken har den endast läsrättigheter, vilket betyder att det inte går att ändra i texten samtidigt. Däremot går det att välja att återställa till en tidigare version på samma plats. Om datorskärmen filmas när detta görs går det att visa att inga ändringar har gjorts.

Dokument som fortfarande finns i papperskorgen går att få ut ur både Office 365 och Google Apps. I Google Apps går det att hämta dokumentet direkt ur papperskorgen utan att göra några ändringar. I Office 365 däremot behöver dokumentet återställas så det inte ligger kvar i papperskorgen. Då har förändringar gjorts i molntjänsten och det ser inte ut på samma sätt som innan.

5.2. Forensisk undersökning av nedladdad data från molntjänster

Ett stort problem då data som har laddats ned från molntjänster undersökts är datumstämplarna. Dokument som tas ut från både Google Apps och Office 365 kommer att få felaktiga datumstämplar. Tidpunkten som står i datumstämpeln för då dokumentet ska ha skapats kommer gälla den tidpunkt dokumentet togs ut istället. Den enda datumstämpeln som stämmer är då dokumentet senast ändrades. Det datumet blir då väldigt viktigt. Det måste vara en tidpunkt som är äldre än då filen skapades för att visa att inget har ändrats i dokumentet efter att det togs ut. Det är även viktigt att de tre andra datumstämplarna har den tidpunkt då dokumenten togs ut. De får inte ha en senare tidpunkt, för då har ändringar skett efteråt.

Även vilken tidszon något skedde i kan bli problem. EnCase skriver inte ut i vilken tidszon en tidpunkt gäller. Det är viktigt att veta i vilken tidszon senaste ändringen skedde så att tidpunkten i EnCase stämmer med tidpunkten i molntjänsten. Därför är det extra viktigt att ställa in samma tidszon på datorn som den forensiska undersökningen görs på, som tidszonen som var registrerad i molntjänsten.

Inga förändringar upptäcktes i den information som togs ut ur molntjänsterna. Däremot är det svårt att säga helt säkert att inget i innehållet förändrades. Det går inte att ta hashsummor för att se om förändringar skett eller inte, eftersom filerna inte är uppbyggda på samma sätt i molnet som på datorn då de tagits ut. Det enda sättet dokumenten jämfördes mellan hur de såg ut innan och efter de hade tagits ut var genom verktyg som jämför textsträngar. På så vis gick det att utesluta att förändringar skett i dokumentens text.

5.3. Forensisk undersökning av dator som använt molntjänster

Väldigt mycket data sparas på datorn när molntjänster används. På samma sätt som data sparas när en användare besöker hemsidor sparas data när användning av molntjänst sker via webbläsaren.

Ibland går det att hitta mycket information från webbläsarna och ibland mindre, beroende på vad som sparats eller inte. I detta arbete har endast en dator som använt molntjänster undersökts. För att säkerställa exakt vad varje webbläsare sparar måste flera tester göras på fler datorer och vid större användning. Resultatet har visat att en hel del information sparas på datorn efter användning. Speciellt gäller detta dokument och e-post. Kontakter och möten i kalendern sparades inte i samma utsträckning.

Ur forensisk synvinkel är det mycket sämre om en användare använder sig av molntjänster än program på datorn. Detta gäller främst då utredaren inte har

användaruppgifter hos molntjänsten och behöver få ut informationen från datorn. Mer data kan döljas från den som undersöker datorn vid användning av molntjänst.

För både dokument och e-post var det väldigt stor variation för vad som hittades mellan de olika webbläsarna. Det varierade även mellan de två tjänsterna Office 365 och Google Apps, eftersom de är uppbyggda på olika sätt hanterar webbläsarna dem annorlunda.

När det gäller datan från deras offlinetjänster hittades de dokument som inte hade raderats enkelt från Google Apps, medan endast rubriken från dokument i Office 365 hittades. Google Apps tar bort raderade dokument ur offlinetjänsten då de inte ska gå att nå av användaren offline och då tas de även bort ur filen som sparar innehållet på datorn. Dokumentet raderas helt från filen och går då inte att hitta när datorn undersöks. Den kan dock finnas kvar i det oallokerade utrymmet om inget annat har skrivit över det.

Dokumenten i Office´s offlinetjänst sparade inte innehållet i dokumenten i klartext och gick därför inte att hitta då datorn undersöktes. Om en liveundersökning skulle göras av datorn och programmet SharePoint Workspace skulle öppnas upp skulle det går att få ut all data.

Skulle användaren ha använt program på sin dator och sparat alla filer på datorn istället för i en molntjänst hade mycket mer information hittats direkt på datorn än vad som nu identifierades.

5.4. Begränsningar av studien

Då den forensiska undersökningen av en dator som använt molntjänster gjordes så testades detta endast på en dator. För att få ett säkrare resultat så behöver flera datorer undersökas och molntjänsterna måste användas mer i varje webbläsare.

Det var även svårt att kunna jämföra dokument som hade tagits ut ur molntjänsterna för att se om förändringar gjorts. Eftersom det inte går att använda hashsummor måste jämförelser göras på andra sätt. Det enda som gjordes nu var att jämföra textsträngarna från dokumenten och tidstämplar.

6. Slutsats

Det blir viktigare och viktigare för IT-forensiker att inte endast undersöka den fysiska datorn efter bevis. Färre bevis kommer att finnas på datorn och fler kommer att finnas hos olika tjänster som nås över Internet framöver. Informationen kommer att finnas spridd bland olika leverantörer. Därför är det fortfarande viktigt att undersöka den fysiska datorn för att se vilka program och tjänster som har använts. Sedan är det inte säkert att bevisen finns på datorn men då vet utredaren var bevisen kan finnas, genom att veta vilka tjänster som har använts.

Ur forensisk synvinkel är det mycket sämre om en användare använder sig av molntjänster än program på datorn. Det gäller främst då utredaren inte har användaruppgifter hos molntjänsten och behöver få ut all information från användarens dator. Mer data kan döljas från den som undersöker datorn om en molntjänst har använts till skillnad mot vanliga program på datorn.

Vid motsatta förhållanden, när det endast finns tillgång till användarens inloggningsuppgifter hos molntjänsten, men inte tillgång till datorn kan all data tas ur molntjänsten. Även om det är mer komplicerat att få ut det på ett korrekt sätt. Det går nämligen inte bara att ta en kopia på all information som finns lagrad för användaren hos molnleverantören, utan varje del måste tas ut var för sig. All data finns inte heller på samma plats och det syns inte alltid tydligt om det är möjligt att få ut det som efterfrågas ur molntjänsten.

Ett problem med att ta ut information från en aktiv tjänst istället för att ta informationen från en kopia är att datan kan förändras under tiden den tas ut. Därför är det viktigt att ta ut informationen i rätt ordning och att användarkontot låses från användaren. Loggar om användarens aktivitet måste tas ut först, innan utredaren loggar in på användarkontot och tar ut resterande informationen.

Det bästa skulle vara om molnleverantörer erbjuder att ta ut all information som rör en användare. Att de då skulle erbjuda detta som en tjänst inom sin molntjänst, så att det enkelt skulle gå att få ut all information som rör en användare på ett säkert och snabbt sätt. På så sätt skulle det inte vara möjligt att påverka information då den tas ut. Google är på god väg genom deras tjänst Google Takeout och föreningen dataliberation.org. Däremot handlar det främst om hur dokument och andra filer kan tas ut och mindre om metadata och loggar som kan vara viktiga ur forensisk perspektiv.

Det är även väldigt svårt att få ut metadatan, speciellt för dokument. Vem som har gjort ändringar och när de gjordes är information som lagras men som är svår att få ut. Samma gäller information om vilka personer som har tillgång till dokument då de delas mellan flera användare. Som det är idag behöver ett dokument i taget markeras och valet att få mer information väljas om det specifika dokumentet. Det är väldigt tidskrävande om många dokument ska undersökas, att göra samma procedur om och om igen. För att kunna behålla den informationen behöver datorskärmen filmas under tiden.

Om det skulle gå att få ut all data genom en tjänst skulle det vara enklare och säkrare än det är idag. Som det är nu är det viktigt att datorskärmen filmas samtidigt som informationen tas ut för att kunna bevisa att inga förändringar gjorts. Annars är det svårt att bevisa det.

Användningen av molntjänster har gjort det mer komplicerat då forensiska utredningar görs. Däremot finns det även goda förutsättningar om de företag som säljer molntjänster

är villiga att ge ut informationen om sina användare genom en tjänst. Det kan bli både enklare och tillförlitligare än vad det är idag att få ut all information från en molntjänst.

7. Avslutning

7.1. Framtida arbeten

Google Apps håller just nu på att göra om Google Docs till deras nya tjänst Google Drive. Vad skillnaderna är mellan tjänsterna har inte undersökts. Vissa delar av resultatet som gäller dokument kan komma att ändras i Google Drive. Främst verkar synkroniseringen med dokument som finns sparade lokalt på datorn förändras. Om en forensisk undersökning ska göras där Google Drive finns istället för Google Docs, behöver skillnaderna först undersökas.

I Google Apps är det möjligt att använda deras API och bygga ihop ett eget program som hämtar ut all data och tar med metadata för dokument. [33] Att ha ett eget program som hämtar ut all information från en tjänst skulle göra arbetet snabbare och kanske även säkrare, beroende på hur datan hämtas ut.

I Office 365 skiljer det sig mycket mellan vilket version som används. I detta arbete undersöktes inte de loggar som går att få ut då ”Office 365 – alternativ E1” används. Det ska då gå att få ut vem som öppnat, ändrat och raderat ett dokument. Exakt hur mycket information det går att få ut och hur detta görs skulle behöva undersökas djupare.

Dessa molntjänster utvecklas väldigt snabbt och förändringar sker hela tiden. Därför kan den specifika informationen om hur det ska göras komma att förändras. Detta gäller främst bilaga 2 som är en guide. Då forensiska undersökningar ska göras måste utredaren hela tiden vara uppdaterad med den senaste tekniken och veta vad som skiljer de nyare versionerna mot de äldre.

En viktigt del som måste undersökas som inte har tagits upp i detta examensarbete är hur det ska fungera juridiskt när datan finns sparad i ett annat land eller i flera olika länder. Det är viktigt att utreda hur inhämtningen av data ska ske på ett sätt som är förenligt med svensk lag.

8. Referenser

1. Mell, P., Grance, T. (2011) *The NIST Definition of Cloud Computing*, Special Publication 800-145, National Institute of Standards and Technology

2. Lillard, Terrence V (2010), *Digital Forensics for Network, Internet and Cloud Computing*, ”What is Network Forensics?” s. 3, 1 uppl, Syngress Media - ISBN 978-1-59749-537-0

3. Volonino, R., Anzaldua, R. (2008), *Cloud Computing For Dummies*, ”Deleting is a misnomer”, s. 10, 1 uppl, Wiley - ISBN 978-0-47037-191-6

4. Taylor, M., Haggerty, J., Gresty, D., Lamb D. (2011) Network Security, *Forensics investigations in cloud computing systems* – ISSN 1353-4858 – Vol 11, nr 3, s. 5

5. Taylor, M., Haggerty, J., Gresty, D., Hegarty, R. (2010) Computer Law Security Review, *Digital evidence in cloud computing systems* - ISSN 0267-3469 – Vol 26, nr 3, s. 304 – 308

6. Lillard, Terrence V (2010), ”Digital Forensics for Network, Internet and Cloud Computing”, ”Evidence Collection in the Cloud” s. 274, 1 uppl, Syngress Media, ISBN 978-1-59749-537-0

7. Graphics Software, ”ScreenCams: Screen Recorders for Windows”, About.com, http://graphicssoft.about.com/od/screenrecorders/ScreenCams_Screen_Recorders_for_Windows.htm, 2012-05-22

8. Bilaga 2: Guide\Google Apps\Insamling av data ur molntjänst\Loggar & Statistisk

9. Anna Guo (2012), ”Can I see when a user was blocked?”, Microsoft, http://community.office365.com/en-us/f/150/p/53498/189781.aspx, 2012-05-15

10. Bilaga 2: Guide\Google Apps\Insamling av data ur molntjänst\Loggar & Statistik

11. Jonis Estrem (2012), ”User Login Info – Sharepoint”, Microsoft, http://community.office365.com/en-us/f/152/t/49438.aspx, 2012-05-22

12. Jonis Estrem (2012), ”User Login Info – Sharepoint”, Microsoft, http://community.office365.com/en-us/f/152/t/49438.aspx, 2012-05-22

13. Anna Guo (2012), ”Can I see when a user was blocked?”, Microsoft, http://community.office365.com/en-us/f/150/p/53498/189781.aspx, 2012-05-15

14. Anna Guo (2012), ”Can I see when a user was blocked?”, Microsoft, http://community.office365.com/en-us/f/150/p/53498/189781.aspx, 2012-05-15

15. Anna Guo (2012), ”Can I see when a user was blocked?”, Microsoft, http://community.office365.com/en-us/f/150/p/53498/189781.aspx, 2012-05-15

16. Anna Guo (2012), ”Can I see when a user was blocked?”, Microsoft, http://community.office365.com/en-us/f/150/p/53498/189781.aspx, 2012-05-15

17. Anna Guo (2012), ”Can I see when a user was blocked?”, Microsoft, http://community.office365.com/en-us/f/150/p/53498/189781.aspx, 2012-05-15

18. Jack Sun (2012), ”Can a administrator see user login statistics?”, Microsoft, http://community.office365.com/en-us/f/150/p/49848/174933.aspx, 2012-04-25

19. Microsoft Office, ”Visa granskningsrapporter”, Microsoft, http://office.microsoft.com/sv-se/sharepoint-online-enterprise-help/view-audit-log-reports-HA102039795.aspx, 2012-05-22

20. Bilaga 2: Guide\[Google Apps | Office 365]\Insamling av data ur molntjänst\Tidszon

21. Bilaga 2: Guide\Office 365\Insamling av data ur molntjänst\Dokument\Övrig

dokumentinformation

22. Bilaga 2: Guide\Google Apps\Insamling av data ur molntjänst\Dokument\Övrig dokumentinformation

23. Bilaga 2: Guide\Google Apps\Insamling av data ur molntjänst\Dokument\Övrig dokumentinformation

24. Bilaga 2: Guide\Office 365\Insamling av data ur molntjänst\Dokument\Övrig dokumentinformation

25. Jesper Osgaard (2012), ”What happens if I empty the Recycle Bin”, Microsoft, http://blogs.technet.com/b/lystavlen/archive/2012/03/28/help-i-deleted-a-document-in-sharepoint-online.aspx, 2012-05-22

26. Google Docs, ”Document deletion and recovery policy”, Google, http://support.google.com/docs/bin/answer.py?hl=en&answer=1704883, 2012-05-22

27. Bilaga 2: Guide\Office 365\Insamling av data ur molntjänst\Dokument\Raderade dokument

28. Text Compare, http://text-compare.com, 2012-05-25

29. Carvey, Harlan (2007), ”Windows Forensic Analysis”, s. 231, 2 uppl. Syngress Media, ISBN 978-1-59749422-9

30. Bilaga 2: Guide\[Google Apps | Office 365]\Forensisk undersökning av dator som använt molntjänst\Webbläsardata

31. Bilaga 2: Guide\[Google Apps | Office 365]\Forensisk undersökning av dator som använt molntjänst\Data från offline användning

32. Jim McCoy (2010), ”SharePoint Workspace and the Office Document Cache, Microsoft, http://blogs.msdn.com/b/sharepoint_workspace_development_team/archive/2010/03/12/sharepoint-workspace-and-the-office-document-cache.aspx, 2012-05-22

33. Bilaga 2: Guide\Google Apps\Insamling av data ur molntjänst\Dokument\Övrig dokumentinformation

Bilagor

1. Ordlista

- **Molntjänst/datormoln**

  En teknik där tjänster erbjuds över Internet. Inga program körs på den lokala datorn utan allt körs från leverantören av molntjänsten. Kunder delar på alla resurser, som nätverk, servrar och applikationer.

- **Forensisk undersökning av en IT-miljö**

  Hur identifiering, insamling, undersökning och analysering av data ska ske i digitala miljöer då integriteten samtidigt ska bevaras.

- **Google Apps**

  Webbaserat kontorsverktyg från Google som ska förenkla implementering och underhåll för kunderna, då allt finns i molnet istället för på en lokal dator.

- **Office 365**

  Webbaserat kontorsverktyg från Microsoft.

- **Hashsumma**

  En hashsumma används för att jämföra filer. Den har en fixerad längd och små skillnader i en fil skapar helt olika hashsummor.

- **EnCase**

  Ett forensiskt verktyg för att undersöka datorer.

- **Metadata**

  Data som handlar om data, exempelvis datumstämplar hos dokument.

2. Guide för forensisk undersökning av Office 365 & Google Apps

Innehållsförteckning

1. Översikt

Det här är en guide för hur det praktiskt ska gå till att ta ut forensiskt intressant information ur molntjänster. Denna guide gäller tjänsterna Office 365 från Microsoft och Google Apps från Google. Den är skriven flr att en annan person ska kunna göra om alla stegen och hitta samma information. Notera att den information som är likadan för både Office 365 och Google Apps kommer att finnas i båda kapitlen. Detta för att det ska gå att läsa endast en del av guiden och fortfarande kunna utföra undersökningen.

Guiden är uppdelad i tre delar, insamling av data ur molntjänsten, forensisk undersökning av nedladdad data från molntjänsten och forensisk undersökning av datorn som användes.

De versioner som används för denna guide är:

- Google Apps for Business, april 2012
- Microsoft Office 365 (alternativ P1), april 2012

Ingen av dessa tjänster har ett versionsnummer, därav står månaden då denna undersökning gjordes.

Det specifika domännamnet som har använts vid det praktiska försöken (”sofiawestberg.com”) har i rapportens guide ändrats till ”my-domain.com”. Användarnamn har ändrats till ”username” från ”Admin” & ”Test”.

2. Office 365

2.1. Förarbete

Det första som behöver göras är att få tillgång till domänens administratörskonto för Office 365. Delar av det som ska göras kommer att göras från detta konto, medan annat behöver göras från användarens konto.

Det är viktigt att så fort som möjligt byta lösenord på användarens konto och på så vis låsa ut personen från kontot så att datan inte kan ändras eller raderas. Detta kan administratören göra genom att logga in på administratörskontot och välja ”Admin\Hantering\Användare\Återställ lösenord”.

Beroende på vilken version av Office 365 som används, ingår olika tjänster. För att ta reda på vilken tjänst som används, logga in som administratör och välj ”Admin\Prenumerationer\Licenser”. På www.microsoft.com/sv-se/office365/plans.aspx finns information om vad de olika versionerna av Office 365 innehåller. Det är viktigt att veta vilken version som används eftersom mängden loggar som går att få ut beror på vilken version av Office 365 som används.

Information behöver även samlas in från användarens fysiska dator.

2.2. Insamling av data ur molntjänst

Arbetet i detta kapitel bör göras vid en dator anpassad för användning vid forensiska undersökningar. Den här delen ska alltså inte göras på den dator som tillhör den användare som undersöks.

2.2.1. Loggar & Statistik

Om domänen använder ”Microsoft Sharepoint Online for Enterprises” och ”Sharepoint Server” för användarna, går det att få ut loggar om vem som öppnat, ändrat, raderat och gjort ändringar i filer samt ändringar av rättigheter. [1, 2] Dessa tjänster ingår idag i ”Microsoft Office 365 – alternativ E1”, vilket är tjänsten för medelstora verksamheter och företag. [3]

Observera att det genom detta inte går att se när en användare senast loggade in på sitt konto, detta är idag inte möjligt i Office 365. [4]

Däremot går det att se när användaren senast loggade in på Outlook i Office 365 och läste sin e-post, kalender, kontakter eller uppgifter. Men om användaren endast loggar in på Office 365 (login.microsoftonline.com) och väljer ”Gruppwebbplats” där dokument finns kommer inte senast inloggningstillfälle att uppdateras.

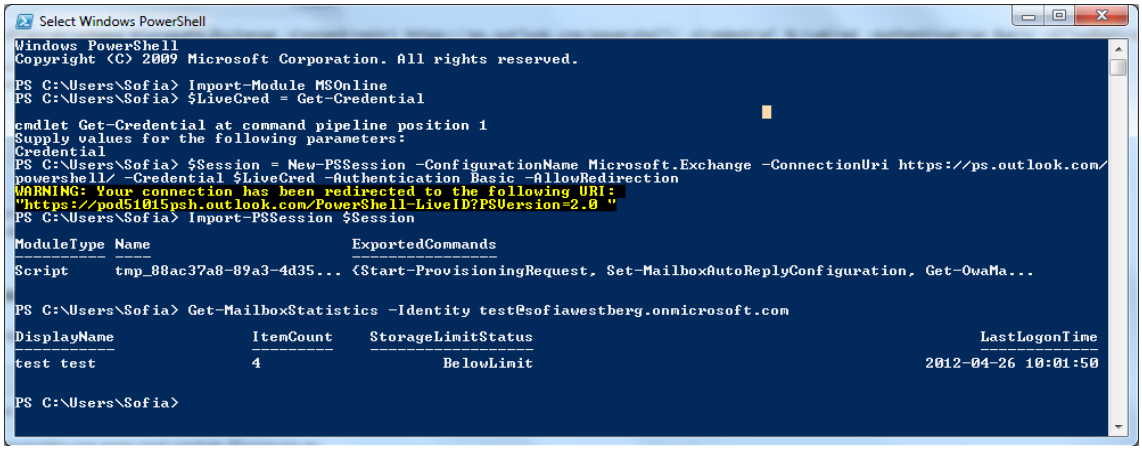
För att se när en användare senast loggade in på Outlook behöver Windows PowerShell användas som är ett kommandorad- och scriptspråk för systemadministration. [5]

För att Windows PowerShell ska fungera för Office 365, följ nedan steg:

- Installera cmdlet för Office 365 [6]
- Installera Microsoft Online Services – inloggningsassistent [7]
- Anslut Windows PowerShell till Microsoft Online Services [8]
- Anslut Windows PowerShell till Office 365 [9]

För tydligare beskrivningar för exakt hur ovan program ska installeras och tjänsterna ska anslutas se källhänvisningarna.

När Windows PowerShell väl fungerar för domänens Office 365 behöver endast kommandot ”Get-MailboxStatistics -Identity username@my-domain.com” anges för att se datum och tid då senast inloggning till Outlook skedde. [10] Se figur 1 för både de kommandon som behövs för installation och det kommando som behövs för att få ut det datum då en användare senast var inloggad.



Figur 1 ”Get-MailboxStatistics”.

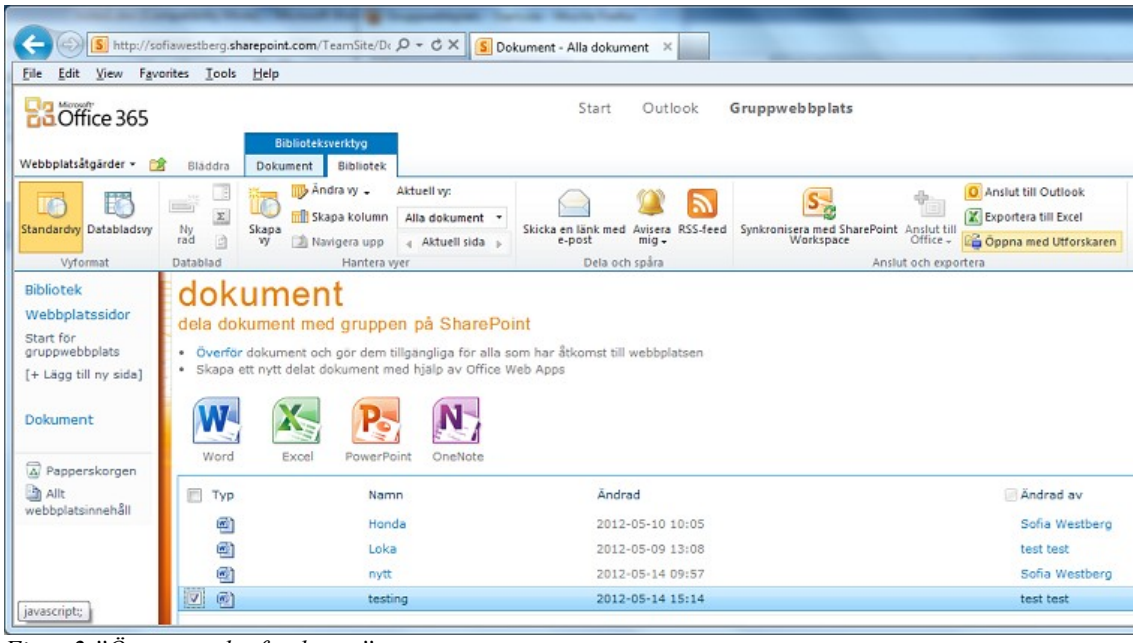
2.2.2. Tidszoner

Det är viktigt att veta vilken eller vilka tidszoner som gäller för användaren. I Office 365 ställs inte tidszoner in automatiskt för användare. Vid första inloggningen får användaren själv välja vilken tidszon som ska användas. [11] För att se vilken tidszon ett användarkonto har inställt, logga in på användarkontot och välj ”Gruppwebbplats\Användarinställningar\Mina inställningar\Mina nationella inställningar\Tidszon”.

2.2.3. Dokument

För att få ut dokument och filer från eventuell webbplats, logga in på det användarkonto som undersöks i Internet Explorer och välj ”Gruppwebbplats\Biblioteksverktyg\Bibliotek\Öppna med utforskaren”. Då öppnas filhanteraren med alla dokument. Observera först om det finns raderade dokument och läs då kapitel 2.2.3.1 ”Raderade dokument” innan fortsättning med att ta ut dokumenten sker.

Fliken ”Biblioteksverktyg” syns inte alltid. För att den ska synas behöver ibland ett dokument markeras, se figur 2.



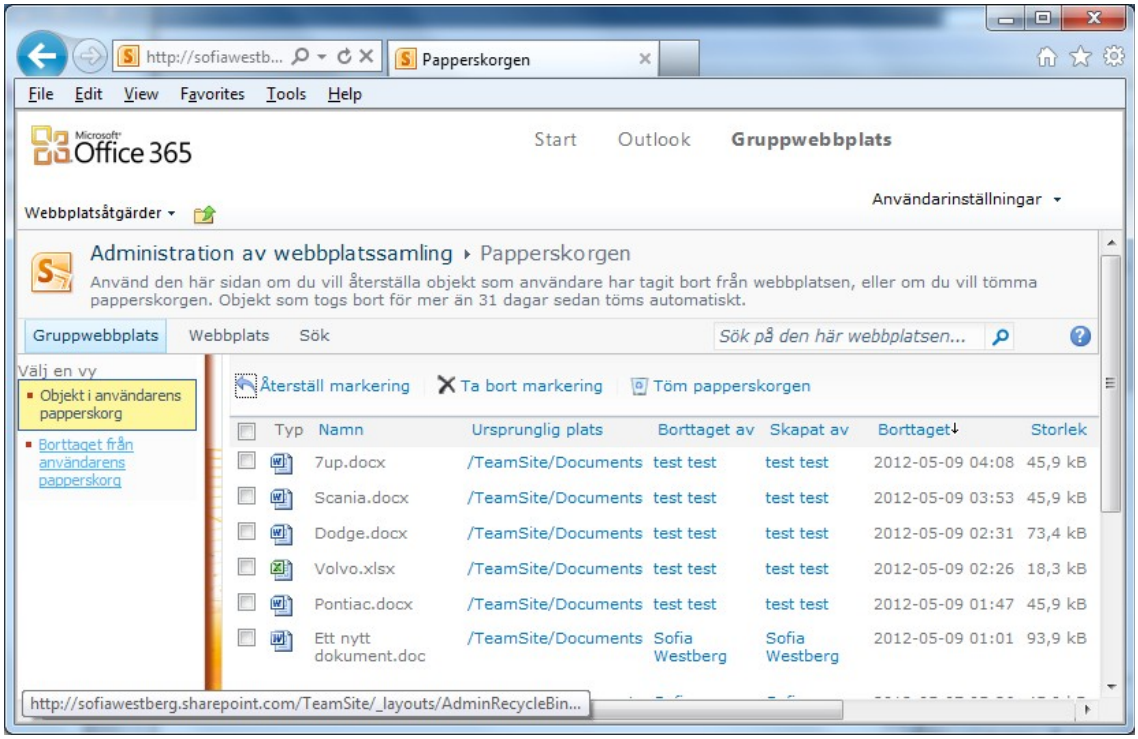
Figur 2 ”Öppna med utforskaren”.

2.2.3.1. Raderade dokument

Raderade dokument går inte att få ut genom samma metod som när vanliga dokument tas ut utan de behöver först återställas för att fås ut. Efter att de har återställts är det möjligt att ta ut alla dokument enligt metoden ovan så att alla dokument tas ut samtidigt.

Innan raderade dokument återställs bör det undersökas vilka dokument som raderats av användaren. I användarens egen papperskorg går det inte att se om det var användaren som raderade dokumentet, utan alla dokument som användaren har behörighet till syns där. Det behöver istället göras från administratörskontot genom att gå in i ”Gruppwebbplats\Papperskorgen” och välja ”Papperskorgen för

webbplatssamling\Objekt i användarens papperskorg”. Den kan administratören annars komma till genom att ange följande webbadress, my-domain.sharepoint.com/_layouts/AdminRecycleBin.aspx. Där visas tydligt vem som skapat och raderat alla raderade dokument i domänen, se figur 3.



Figur 3 ”Administratörspapperskorgen”.

Dokument kan även återskapas efter att de har raderats från användarens papperskorg. Detta beror på att de hamnar i en annan papperskorg hos administratören då de har raderats från användarens papperskorg. Denna går att komma åt på samma sätt som ovan papperskorg men välj sedan ”Borttaget från användarens papperskorg”. Totalt sett sparas dokument i de båda papperskorgarna i högst 30 dagar. [12]

All återställning av raderade dokument kan göras från administratörens konto istället för att göras från den användaren som undersöks. När ett raderat dokument återställs kommer det tillbaka till den plats det raderades ifrån, alltså användarens bibliotek om det var därifrån det raderades.

2.2.3.2. Övrig dokumentinformation

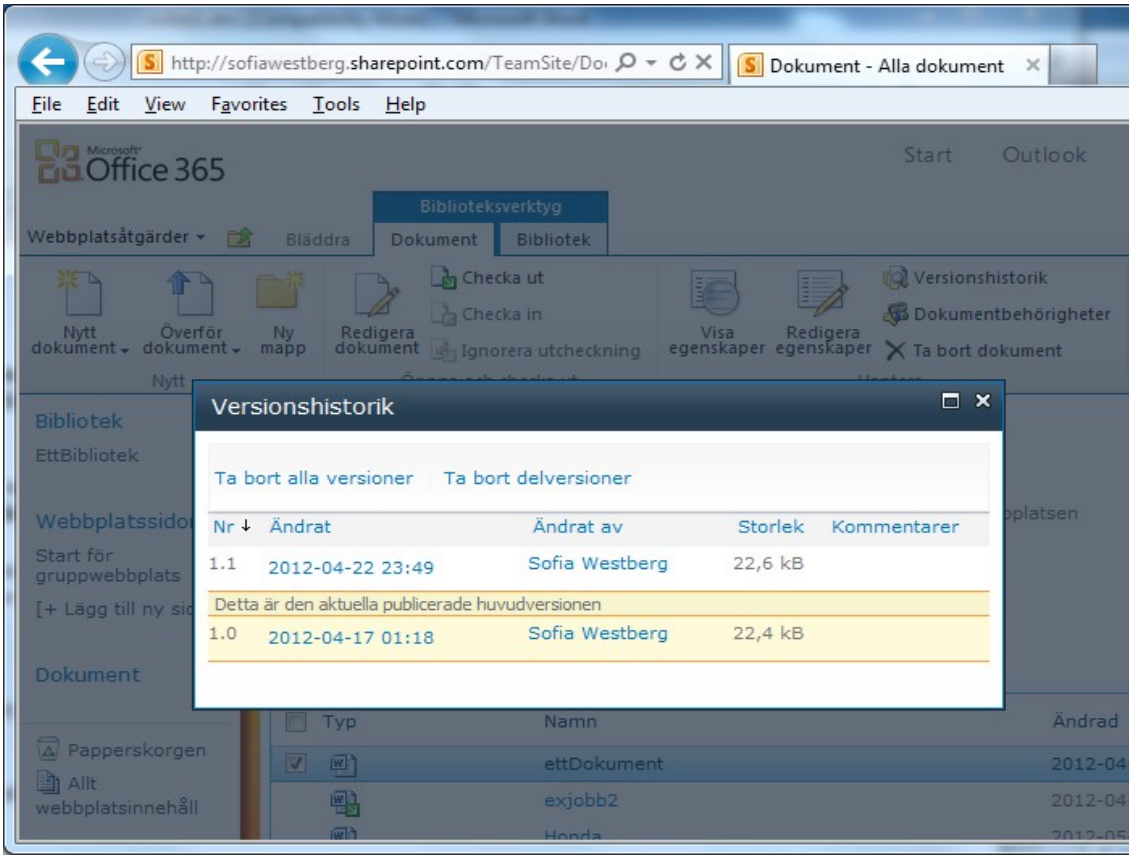
När ett dokument tas ut ur Office 365 kommer datumstämpeln för när dokumentet skapades att gälla tidpunkten det togs ut. Det enda datum som går att få med från dokumentet är den tidpunkt det senast skrevs i dokumentet. Därför är det viktigt att även ta ut information om när dokumentet skapades.

För att se vem som skapat ett dokument och vilket datum det skedde, markera ett dokument i ”Gruppwebbplats” och välj sedan ”Biblioteksverktyg\Dokument\Visa egenskaper”.

För att se när ett dokument blivit ändrat, gå in på ”Versionshistorik” under ”Dokument”. Då visas fler versioner av samma dokument. Däremot behöver detta vara aktiverat sedan innan av administratören för det specifika biblioteket, annars kommer inte historiken att sparas. Utan att behöva öppna upp en gammal version så går det att se vilka användare

som har skapat varje version, se figur 4. På så sätt går det att se vilka som har ändrat i ett dokument.

Notera att en användare har möjlighet att radera tidigare versioner. Det går dock endast att välja att radera alla tidigare versioner. Om detta är syns det att den första versionen (0.1 eller 1.0) saknas.



Figur 4 ”Versionshistorik”.

Problemet med versionshistorik i Office 365 är att det inte går att ta ut äldre versioner av ett dokument utan att återställa dokumentet till den versionen. Om det finns ett dokument med versionerna 1.0, 2.0 & 3.0 och det är version 2.0 so ska undersökas behöver den versionen återställas. Då blir den version 4.0. På så vis går det fortfarande att gå tillbaka till den riktiga versionen (3.0), men detta kommer att ändra i dokumentet. [13]

För att se vilka som har behörighet att ändra i ett dokument, välj ”Dokumentbehörigheter” i ”Biblioteksverktyg\Dokument”. Eftersom de flesta dokument och bibliotek som finns i ”Gruppwebbplats” delas mellan alla användare behöver inte dokument vara lästa av användaren bara för att de finns i ”Gruppwebbplats”. Det går inte att se om en användare har öppnat ett dokument.

2.2.4. E-post

För att få ut en användares e-post behöver den läggas till i en e-postklient. För att få fram informationen som behövs för detta, logga in på Office 365 på administratörskontot (för att påverka användarens konto så lite som möjligt). Välj sedan ”Outlook\Alternativ\Visa alla alternativ\Konto\Mitt konto\Inställningar för åtkomst via

POP, IMAP och SMTP”. Denna information kommer att vara densamma för alla inom samma domän.

När e-posten är upplagd i en e-postklient kan e-posten tas ut på samma sätt som e-post tas ut vid vanliga forensiska undersökningar av datorer då e-postklienter används.

2.2.5. Kontakter

Kontakter går att få ut genom att logga in på Office 365, välja ”Outlook\Kontakter”, markera alla kontakter och välja ”Vidarebefordra som bifogad fil”. Då kan ett e-postmeddelande skickas med alla kontakter. Kontakterna läggs då i separata vcf-filer.

Kontakter kan även erhållas via en e-postklient på samma sätt som för e-posten.

2.2.6. Kalender

Kalendern går att få ut genom att logga in på Office 365, välja ”Outlook\Kalender” och klicka på symbolen med en skrivare på. Det går att välja mellan att skriva ut en dag, vecka eller månad i taget. Observera att det går att välja mellan vilka klockslag som möten ska tas med, standard är endast dagtid (08:00 – 17:00). För att försäkra sig om att alla möten kommer med måste 0:00 – 0.00 väljas. Sedan går det även att välja ”Skriv ut detaljerad dagordning tillsammans med kalendern”, då kommer en bilaga med alla datum och dess möten med.

Kalendern kan även erhållas via en e-postklient på samma sätt som för e-posten.

2.3. Forensisk undersökning av nedladdad data från molntjänst

När datan väl har tagits ut från Office 365 ska den undersökas på samma sätt som när en vanlig forensisk undersökning görs av en dator. Datan tas då in i ett program för forensiska undersökningar, som EnCase eller Forensic Toolkit.

2.4. Forensisk undersökning av dator som använt molntjänst

För detta kapitel görs en forensisk undersökning av den eller de enheter som använts för att komma åt molntjänsterna av användaren.

2.4.1. Webbläsardata

Olika webbläsare lagrar användardata på olika platser. Nedan går det att se var de olika webbläsarna lagrar den användardata som gäller för Office 365 i Windows 7.

Google Chrome	C:\Users\username\AppData\Local\Google\Chrome\User Data
Mozilla Firefox	C:\Users\username\AppData\Local\Mozilla\Firefox\Profiles
Microsoft Internet Explorer	C:\Users\username\AppData\Local\Microsoft\Windows

2.4.2. Data från offline användning

En användare kan komma åt dokument m.m. från Office 365 offline om den har Microsoft SharePoint Workspace installerat på datorn. Detta ingår i Microsoft Office Professional Plus. Filerna sparas inte i en mapp på datorn som enkelt går att komma åt

från filhanteraren utan de går endast att komma åt dem genom programmet.

SharePoint Workspace synkroniserar var 10:e minut mot Office 365, vilket betyder att det kan finnas data här som inte syns när inloggning på användarens konto sker. [14] Speciellt om användarens dator inte har varit uppkopplad mot Internet på ett tag kan den ha äldre versioner av dokument, eller raderade dokument som finns kvar.

Rubrikerna från dokument i SharePoint Workspace kan hittas i ”C:\Users\username\AppData\Local\Microsoft\Office\Groove”. Groove är det namn som SharePoint Workspace hade i tidigare versioner av Windows. Det går även hitta rubrikerna i ”C:\Users\username\AppData\Local\Microsoft\Office\14.0\OfficeFileCache”. Däremot går det inte få fram innehållet från dokumenten när en forensisk undersökning görs av datorn. För att få ut innehållet i dokumenten behöver programmet SharePoint Workspace vara igång.

3. Google Apps

3.1. Förarbete

Det första som behöver göras är att få tillgång till domänens administratörskonto för Google Apps. Delar av det som ska göras kommer att göras från detta konto, medan annat behöver göras från användarens konto.

Det är viktigt att så fort som möjligt byta lösenord på användarens konto och på så vis låsa ut personen från kontot så datan inte kan ändras eller raderas. Detta görs från administratörskontot med valen ”Organisation & användare\Lösenord\Ändra lösenord”.

Information behöver även samlas in från användarens fysiska dator.

3.2. Insamling av data

Arbetet i detta kapitel bör göras vid en dator anpassad för användning vid forensiska undersökningar. Den här delen ska alltså inte göras på den dator som tillhör den användare som undersöks.

3.2.1. Loggar & Statistik

I Google Apps går det som administratör att få ut en del statistik om användarnas användning av Google Apps tjänster. Loggarna går att få fram genom att logga in på administratörskontot och välja ”Rapporter\Användning & Rapporter”.

I tabell 1 nedan finns de loggar som kan vara intressanta ur ett forensiskt perspektiv för Google App.

Användning & Rapporter	
Användningsgraf	Inga användarspecifika loggar, men statistik om hur många användare som använt en specifik tjänst under en viss period.
Granskningsrapporter	Datum när användare har skapats, ändrat lösenord, raderats, aktiverats och blockerats. Även datum för en del inställningar hos administratören som har ändrats, t.ex. när tidszonen senast ändrades. Denna logg kan filtreras på exempelvis en e-postadress.
Ytterligare Rapporter	Främst statistik över alla användare, som antal aktiva användare under en månad. Valet ”Kontorapport” får fram information om varje användarkonto specifikt, bland annat information om datum kontot skapade, senaste inloggningen och om kontot är aktivt eller avstängt.

Tabell 1 ”Användning & Rapporter”.

Alla rapporter kan erhållas som csv-filer.

3.2.2. Tidszoner

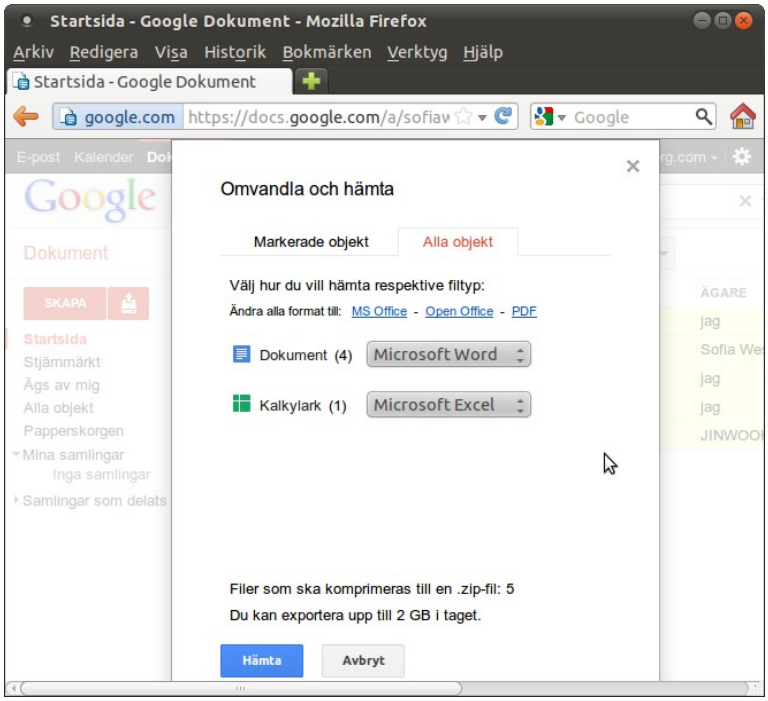
Det är viktigt att veta vilken eller vilka tidszoner som gäller för användaren. För att ta reda på detta, logga in på administratörskontot och välj ”Domäninställningar\Allmänt\Tidszon”. Det är denna tidszon som sätts som standard för alla användare. I ett antal av Googles tjänster går det även att ändra tidszon i den specifika tjänsten (ex. dokument, kalender, sites). För att se om en tidszon är ändrad i en tjänst, logga in på användarkontot och klicka på kugghjulssymbolen uppe i högra hörnet på den specifika tjänsten. Finns det ett val för tidszon bör den noteras, annars är tidszonen den som finns som standard på administratörskontot.

3.2.3. Dokument

Alla dokument tas enklast ut genom att använda tjänsten Google Takeout. Logga in på användarkontot på www.google.com/takeout, välj ”Skapa arkiv” och ”Ladda ned” för att få alla dokument i en zip-fil. Se till att det är valt ”All av din data” och inte en specifik tjänst vald. På detta sätt går det att få ut mer än användarens dokument, om användaren använt sig av Google + eller Picasa Web Albums går det att få data från dessa tjänster också.

Det är viktigt att notera att dokument som skapas i Google Apps inte har en filändelse då de skapas (t.ex. .doc eller .odt). Utan de skapas i Googles egna format. När dokumenten tas ut genom Google Takeout kommer de att göras om till det format som är satt som standard för kontot.

Det går även att välja att hämta dokumenten genom att logga in på användarens konto på docs.google.com, markera alla dokument och välja ”Mer\Hämta\Alla objekt”, se figur 5. Då går det att välja vilket filformat det ska vara för de dokumenten, exempelvis .doc, .pdf eller .odt. För att vara säker på att alla dokument kommer med är det viktigt att välja just ”Alla objekt” även om alla objekten är markerade redan, på så sätt ingår dokument som kan finnas i andra mappar också.



Figur 5 ”Hämta dokument”.

3.2.3.1. Raderade dokument

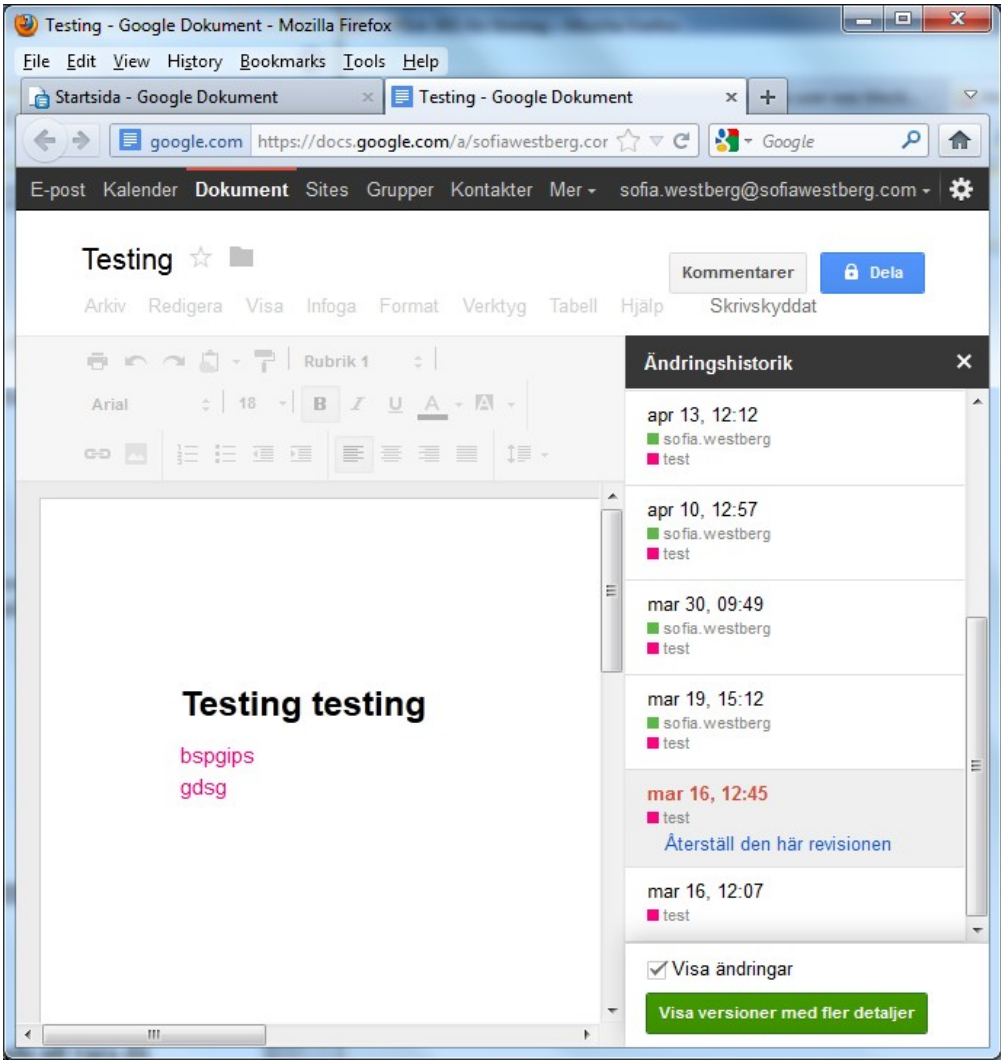
För att hämta ut raderade dokument, logga in på användarens konto på Google Docs. Välj sedan ”Papperskorgen”, markera alla dokument och välja ”Mer\Hämta\Alla objekt”.

Det går inte att återskapa dokument som raderats från papperskorgen. [15]

3.2.3.2. Övrig dokumentinformation

När ett dokument tas ut ur Google Apps kommer datumstämpeln för då dokumentet skapades att vara då dokumentet togs ut. Det enda datum som går att få med från dokumentet är då det senast ändrades i dokumentet. Därför är det viktigt att även ta ut information om när dokumentet skapades.

Det datum ett dokument skapades och vem som gjorde det går endast att se genom att gå in i dokumentet i Google Docs och välja ”Arkiv\Se Omarbetningshistorik”, som visas i figur 6. Välj sedan ”Visa versioner med fler detaljer” för att få exakta datumet och klockslaget som första ändringen gjordes. Om detta väljs kommer de första ändringarna att slås ihop. Då kan den senaste tidpunkten ett dokument ändrades under en dag visas, istället för den första tidpunkten.



Figur 6 ”Historik”.

Även om en användare står som enda ägare på ett dokument betyder inte det att användaren har öppnat eller läst dokumentet. En annan användare kan ge användaren dessa rättigheter och ta bort sina egna rättigheter. I ”Se Omarbetningshistorik” går det att se alla som har ändrat i ett dokument och på så sätt se om användaren faktiskt har skrivit i dokumentet. Den som senast ändrade i ett dokument syns även i ”Förhandsgranska”, för att se det, markera ett dokument och klicka på symbolen med ett öga.

Där går det även att se vem som är ägare och vilka som får redigera eller läsa i dokument. Om en sökning görs på Internet av en användare och den hittar information som finns i ett Google Dokument som sedan öppnas kommer det att hamna bland dess egna dokument i Google Docs. Alla dokument som går att få upp på detta sätt har valet ”Publicera på webben” i ”Förhandsgranska\Synlighet”.

Det går även att få ut all historik genom Google Document List API. [16] Då går det att få ut historiken som finns i ”Se Omarbetningshistorik”. Ett API låter programmerare att skapa egna applikationer som läser och skriver data till en tjänst, som här till Google Docs.

3.2.4. E-post

För att få ut en användares e-post behöver den läggas till i en e-postklient. För att få fram informationen som behövs för detta, logga in på mail.google.com som administratör (för att påverka användarens konto så lite som möjligt). Klicka sedan på kugghjulssymbolen och välj ”Inställningar\Vidarebefordran och POP/IMAP”. Under ”IMAP-åtkomst”, välj ”Aktivera IMAP” och klicka på ”Anvisningar för konfigurering” för att se vilka inställningar som behövs.

När e-posten är upplagd i en e-postklient kan e-posten tas ut på samma sätt som e-postmeddelanden tas ut vid vanliga forensiska undersökningar av datorer då e-postklienter används.

3.2.5. Kontakter

Kontakter går att få ut genom att logga in på användarens konto på www.google.com/contacts, markera alla kontakter och välja ”Mer\Exportera”. Då går det att välja tre olika format att exportera kontakterna till, Google CSV, Outlook CSV och vCard (.vcf).

Kontakter kan även erhållas via en e-postklient på samma sätt som för e-posten.

3.2.6. Kalender

För att få ut kalendern, logga in på användarens konto på www.google.com/calendar och välj ”Fler\Skriv ut”. Sedan går det att antingen välja att skriva ut kalendern eller hämta den som pdf. Den kommer då ut med en vecka per sida.
Kalendern kan även erhållas via en e-postklient på samma sätt som för e-posten.

3.3. Forensisk undersökning av nedladdad data från molntjänst

När datan väl har tagits ut från Office 365 ska den undersökas på samma sätt som när en vanlig forensisk undersökning görs av en dator. Datan tas då in i ett program för

forensiska undersökningar, som EnCase eller Forensic Toolkit.

3.4. Forensisk undersökning av dator som använt molntjänst

För detta kapitel görs en forensisk undersökning av den eller de enheter som använts för att komma åt molntjänsterna av användaren.

3.4.1. Webbläsardata

Olika webbläsare lagrar användardata på olika platser. Nedan går det att se var de olika webbläsarna lagrar den användardata som gäller för Google Apps i Windows 7.

Google Chrome	C:\Users\username\AppData\Local\Google\Chrome\User Data
Mozilla Firefox	C:\Users\username\AppData\Local\Mozilla\Firefox\Profiles
Microsoft Internet Explorer	C:\Users\username\AppData\Local\Microsoft\Windows

3.4.2. Data från offline användning

Användare kan läsa dokument som finns i Google Docs även då den inte är uppkopplad mot Internet om webbläsaren Chrome används och applikationen ”Google Docs” är installerad i Chrome.

Användaren behöver då ha tillåtit offline användning för att det ska gå att se dokumenten offline. Det går då att se dokumenten offline genom att gå in på docs.google.com genom webbläsaren Chrome. Även om ingen Internetanslutning finns går det att se de dokument som finns. En användare kan inte redigera eller radera dokument när den är offline, endast läsa dem.

Dokumenten sparas i en fil som finns lokaliserad på ”C:\Users\username\AppData\Local\Google\Chrome\User Data\Default\databases”. Filen som innehåller alla dokument och deras innehåll heter “1”. Filen är av formatet ”SQL Lite 3”. Om filen öppnas i programmet SQLite Spy går det att fram alla dokumentens namn. [17]

Filen innehåller även alla texter som finns i dokumenten. Även raderade dokument kan finnas kvar. När ett dokument raderas från Google Docs uppdateras inte offline tjänsten på en gång, det tar ca. 10 minuter. Däremot sker uppdatering om dokument ändras och läggs till fort.

4. Referenser

1. Microsoft Office, ”Visa granskningsrapporter”, Microsoft, http://office.microsoft.com/sv-se/sharepoint-online-enterprise-help/view-audit-log-reports-HA102039795.aspx, 2012-05-20

2. Microsoft Office, ”Konfigurera granskningsinställningar för en webbplatssamling”, Microsoft, http://office.microsoft.com/sv-se/sharepoint-online-enterprise-help/configure-audit-settings-for-a-site-collection-HA102031737.aspx, 2012-05-20

3. Microsoft Office 365, ”Alternativ och priser”, Microsoft, http://www.microsoft.com/sv-se/office365/plans.aspx, 2012-04-16

4. Jonis Estrem (2012), ”User Login Info – Sharepoint”, Microsoft, http://community.office365.com/en-us/f/152/t/49438.aspx, 2012-05-22

5. Microsoft Windows Server (2008), ”Windows PowerShell”, Microsoft, http://technet.microsoft.com/sv-se/library/cc731851%28v=ws.10%29.aspx, 2012-05-22

6. Microsoft Office 365 (2012) ”Använda Windows PowerShell för att hantera Office 365”, Microsoft, http://onlinehelp.microsoft.com/sv-se/office365-enterprises/hh124998.aspx, 2012-05-22

7. Microsoft Office 365 (2012) ”Använda Windows PowerShell för att hantera Office 365”, Microsoft, http://onlinehelp.microsoft.com/sv-se/office365-enterprises/hh124998.aspx, 2012-04-24

8. Microsoft Office 365 (2012) ”Använda Windows PowerShell för att hantera Office 365”, Microsoft, http://onlinehelp.microsoft.com/sv-se/office365-enterprises/hh124998.aspx, 2012-04-24

9. Microsoft Outlook (2011) ”Ansluta Windows PowerShell till tjänsten”, Microsoft, http://help.outlook.com/sv-se/140/cc952755.aspx, 2012-04-24

10. Microsoft Exchange Server (2011), ”Get-MailboxStatistics”, Microsoft, http://technet.microsoft.com/en-us/library/bb124612.aspx, 2012-04-26

11. Microsoft Support (2011), ”The time zone setting in Outlook Web App in Office 365 is incorrectly set to (UTC) Monrovia, Reykjavik”, Microsoft, http://support.microsoft.com/kb/2298834, 2012-05-17

12. Jesper Osgaard (2012), ”What happens if I empty the Recycle Bin”, Microsoft, http://blogs.technet.com/b/lystavlen/archive/2012/03/28/help-i-deleted-a-document-in-sharepoint-online.aspx, 2012-04-13

13. Jason Burnside (2012), ”Previewing an existing document found in version history”, Microsoft, http://www.community.office365.com/en-us/f/154/p/46943/172590.aspx, 2012-04-13

14. Microsoft Office, ”Synkronisera innehåll i en SharePoint-arbetsyta”, Microsoft, http://office.microsoft.com/sv-se/sharepoint-workspace-help/synchronizing-content-in-a-sharepoint-workspace-HA010374732.aspx, 2012-05-22

15. Google Docs, ”Document deletion and recovery policy”, Google, http://support.google.com/docs/bin/answer.py?hl=en&answer=1704883, 2012-04-03

16. Google Developers. ”Google Document List API: Managing revisions of documents and files”, Google, https://developers.google.com/google-apps/document-list/#managing_revisions_of_documents_and_files, 2012-05-22

17. Delphi Components and Software Applications, ”SQLiteSpy”, Delphi, http://www.yunga.de/delphi/doku.php/products/sqlitespy/index, 2012-05-15

HÖGSKOLAN
DALARNA

Högskolan Dalarna
791 88 Falun
Sweden
Tel 023-77 80 00