MEMORANDUM FOR: Requesting Office 16 Apr 18

|  |  |
| --- | --- |
| SUBJECT: | Forensic Examination Final Report |
|  | Report of Investigation: 0001-LoneWolf-2018 |
|  |  |

1. **EXECUTIVE SUMMARY.**

a. A digital copy of this report can be found on the attached findings disk. It contains hyperlinks that allow the reader to directly access the recovered evidence, relevant information, and/or documents referenced in this report. [Exported Evidence Files](file:///C:\Users\Thelma%20Looms\Desktop\TrilogyEd-Course\Garfunkiel-GeorgiaTech\Lone%20Wolf%20Teacher%20Guide\Exported%20Evidence%20Files), [Tagged Files Listings](file:///C:\Users\Thelma%20Looms\Desktop\TrilogyEd-Course\Garfunkiel-GeorgiaTech\Lone%20Wolf%20Teacher%20Guide\Axiom%20Tagged%20Files%20Listing), and artifact reports from [Axiom](file:///C:\Users\Thelma%20Looms\Desktop\TrilogyEd-Course\Garfunkiel-GeorgiaTech\Lone%20Wolf%20Teacher%20Guide\Axiom%20Example%20Reports) and [Autopsy](file:///C:\Users\Thelma%20Looms\Desktop\TrilogyEd-Course\Garfunkiel-GeorgiaTech\Lone%20Wolf%20Teacher%20Guide\Autopsy%20Example%20Report) are located on the Findings Disk.

b. On 6 Apr 18, Special Agent Alpha requested a Digital Forensic Examination of a laptop computer to recover any and all information pertaining to allegations Mr. Jim Cloudy was planning to attack a town hall meeting held to discuss gun violence.

c. A Search Warrant was approved by Not A. REALJUDGE, United States Magistrate Judge, Eastern District of Virginia authorizing the search of Mr. Cloudy’s residence and the seizure and subsequent Digital Forensic Examination of digital media found within. SA Forensicator, Senior Digital Forensic Examiner (SDFE), Alexandria, VA 22303, concurred the Search Warrant was legally sufficient to conduct the examination as requested within the Laboratory Examination Request.

d. Between 13 Apr 18 - 20 Apr 18, the undersigned conducted a forensic examination of the submitted evidence.

e. Examination revealed the following:

|  |  |
| --- | --- |
| 1 | PowerPoint document titled “Operation 2nd Hand Smoke” depicting travel routes from a gun control event to the airport, Google Street View of the venue, a flight itinerary and a hotel in Indonesia. |
| 5 | Word Documents with content including references to an unspecified plan, firearms, latex gloves, ammunition, non-extradition countries, escape routes, press releases, and views on gun control. |
| 16 | Chrome Autofill artifacts containing keywords associated with firearms and locations. |
| 96 | Chrome Current Tabs artifacts containing keywords associated with gun control, non-extradition countries, firearms, public buildings and cloud storage. |
| 85 | Google Search artifacts containing keywords associated with police response times, gun stores, shooting ranges, smuggling cash, public buildings, and cloud storage. |
| 46 | Pictures depicting anti-gun control topics, flight itineraries, public buildings, travel routes, and hotels in Indonesia. |
| 7 | Bin files containing fragments of a OneNote document referencing willingness to “commit another atrocity”, a “fresh start in Bali”, and “A hundred targets. 2000 bullets. Endless freedom.” |

2. **EVIDENCE EXAMINED.**

The undersigned created a forensic duplicate of the following item for examination.

a. **Exhibit 1:** Laptop, Dell, Model Latitude E6430 ATG, Service Tag: DB2MN22. Evidence Property/Custody Document (EPCD) Item 3   
 Document Number 001-18

3. **DETAILED FINDINGS**.

a. **Exhibit 1:** Examination and analysis of Ex 1 revealed the Solid State Drive was formatted in NTFS. All files are in Coordinated Universal Time (UTC) unless otherwise specified.

(1) An antivirus scan of Ex 1, was conducted using Avast Antivirus; no threats were detected.

(2) An examination of PowerPoint Documents parsed by Magnet Axiom and viewed within Artifact view, revealed one unique Microsoft Office PowerPoint file located within five directories associated with the “jcloudy” user profile. For additional details pertaining to sizes locations and timestamps refer to “[PowerPoint Document.csv](file:///C:\Users\Thelma%20Looms\Desktop\TrilogyEd-Course\Garfunkiel-GeorgiaTech\Lone%20Wolf%20Teacher%20Guide\Tagged%20Files%20Listing\PowerPoint%20Documents.csv)” within the Tagged Files Listing folder.

* Filename: “[Operation 2nd Hand Smoke.pptx](C:\\Users\\Thelma Looms\\Desktop\\TrilogyEd-Course\\Garfunkiel-GeorgiaTech\\Lone Wolf Teacher Guide\\Exported Evidence Files\\Operation 2nd Hand Smoke.pptx)”.
* Slide one is a title page.
* Slide two contains an image of a Town Hall Project event scheduled for Sat April 7, 2018 from 12:30PM to 2:00PM local time at 21030 Whitfield PL, Sterling VA, 20165. The event states two Senators will be in attendance to discuss gun violence. A web search of this address revealed a match for “Cascades Library”.
* Slide 3 contains what appears to be a cropped screen capture of a Google Street View image featuring a red brick building which is a visual match for the Cascades Library.
* Slide 4 contains what appears to be a cropped screen capture of a Google Maps satellite view of the area surrounding the Cascades Library. The satellite view features an orange and blue line most likely resulting from a query for directions to or from the Cascades Library. A yellow box labeled “Park” is located over a parking lot located to the West of Cascades Library. A yellow line is drawn from the “Park” box to the library along the most direct route. The library is marked with a red box. A red line is drawn from the “Park” box to the library in a circuitous route. A green line is drawn from the “Park” box and merges with the directions query route line.
* Slide 5 contains what appears to be a cropped screen capture of a Google maps directions query with turn by turn directions from “21030 Whitfield Place” (Cascades Library) to “Dulles International Airport”.
* Slide 6 contains what appears to be a cropped screen capture of flight information obtained from “KAYAK”. The flight is scheduled to depart on “Sat, Apr 7” at 1:20PM local time from “Washington” and arrive at 4:50PM local time in “Seoul”, then continue on “Sun, Apr 8” at 6:05PM local time from “Seoul” and arrive at 12:10AM at “Denpasar (Bali)”.
* Slide 7 contains what appears to be a cropped screen capture of hotel information pertaining to “Sea Breeze Candidasa” in Candidasa, Indonesia.

(3) An examination of Word Documents parsed by Magnet Axiom and viewed within Artifact view, revealed five unique Microsoft Office Word files, each located within multiple directories associated with the “jcloudy” user profile. For additional details pertaining to sizes, locations and timestamps refer to “[Word Documents.csv](file:///C:\Users\Thelma%20Looms\Desktop\TrilogyEd-Course\Garfunkiel-GeorgiaTech\Lone%20Wolf%20Teacher%20Guide\Tagged%20Files%20Listing\Word%20Documents.csv)” within the Tagged Files Listing folder.

* Filename: “[AIRPORT INFORMATION.docx](file:///C:\Users\Thelma%20Looms\Desktop\TrilogyEd-Course\Garfunkiel-GeorgiaTech\Lone%20Wolf%20Teacher%20Guide\Exported%20Evidence%20Files\AIRPORT%20INFORMATION.docx)”.
* “AIRPORT INFORMATION” is a one-page document which contains the following pertinent data:
  + “Ronald Reagan has best record of on-time departures.”
  + “Dulles has flights to Indonesia. With Layover in Qatar.”
  + “22 min from Fairfax County Democratic Committee, 8500 Executive Park Ave, Fairfax, VA 22031 to Dulles Airport.”
  + An apparent screen capture featuring the price of a round trip flight from Washington, DC to Denpasar Bali, Indonesia departing Saturday, April 7, 2018 and returning Saturday, April 21, 2018.
  + The screen capture displays a system time of “2:37AM, 4/3/2018”.
* Filename: “[8537797.docx](file:///C:\Users\Thelma%20Looms\Desktop\TrilogyEd-Course\Garfunkiel-GeorgiaTech\Lone%20Wolf%20Teacher%20Guide\Exported%20Evidence%20Files\8537797.docx)”.
* “8537797” is a two-page document which contains the following pertinent data:
  + Page one is a visually identical to page one of “AIRPORT INFORMATION”.
  + Page two contains an apparent uncropped screen capture which visually matches the image depicted on slide two of “Operation 2nd Hand Smoke.pptx”.
  + The screen capture indicates the event information was obtained from “www.resistancecalendar.org”.
  + The screen capture displays a system time of “2:40AM, 4/3/2018”.
* Filename: “[Cloudy Thoughts (4apr).docx](file:///C:\Users\Thelma%20Looms\Desktop\TrilogyEd-Course\Garfunkiel-GeorgiaTech\Lone%20Wolf%20Teacher%20Guide\Exported%20Evidence%20Files\Cloudy%20thoughts%20(4apr).docx)”.
* “Cloudy Thoughts (4apr).docx” is a one-page document which contains the following pertinent data:
  + “I don’t know if this plan will work. Plans never survive first contact.”
  + “Its going to snow, and the winds will be strong. No problem for the attack, but if my flight is delayed or cancelled, that might prove to be a problem.”
  + “Even if I’m killed at the site, I know that what im doing is just and right.”
  + “I am saving everything to the cloud on several accounts.”
  + “The only record will remain in the cloud and Paul will have the only other keys.”
* Filename: “[Planning.docx](file:///C:\Users\Thelma%20Looms\Desktop\TrilogyEd-Course\Garfunkiel-GeorgiaTech\Lone%20Wolf%20Teacher%20Guide\Exported%20Evidence%20Files\Planning.docx)”.
* “Planning.docx” is a one-page document written in an outline format which contains the following pertinent data:
  + “Must have a good escape route”
  + “Must be in Gun Free zone.”
  + “Gun (black market).
  + “Norther[*sic*] VA Gun Works 7518 Fullerton Rd # K, Springfield, VA 22153”
  + “NOVA 412 W Broad Street Falls Church, VA 22046”
  + “Ammo.”; “9mm is 1000 for $360”; “Kel-Tec Sub 2000 9mm $400.”
  + “Latex gloves”
  + “Velcro tear away clothing?”
  + “Escape”; “No Extradition countries”; “Indonesia (Nicer, but more expensive)”; “Vietnam”; “Can live very well on 100 a day, for 9 years.”
  + ‘”Press Release” once home free.’
* Filename: “[The Cloudy Manifesto.docx](file:///C:\Users\Thelma%20Looms\Desktop\TrilogyEd-Course\Garfunkiel-GeorgiaTech\Lone%20Wolf%20Teacher%20Guide\Exported%20Evidence%20Files\The%20Cloudy%20Manifesto.docx)”.
* “The Cloudy Manifesto.docx” is a seven-page document featuring embedded images with author commentary discussing “safety and protection”, the responsibility to protect one’s self, the role guns play in society, and contains threatening statements.
  + “You will soon see when the blood has been shed and the defenseless bodies stacked high. I will do what I must. No matter who is hurt, the collateral damage will be worth it.”
  + “I will be the change. I will be the revolutionary. I will be the history maker. I will fight. I will be the Lone Wolf.”

(4) An examination of Chrome Autofill records parsed by Magnet Axiom and viewed within Artifact view, revealed 17 artifacts containing keywords associated with firearms and locations associated with the “jcloudy” user profile. For additional details pertaining to sizes locations and timestamps refer to “[Chrome Autofill.csv](file:///C:\Users\Thelma%20Looms\Desktop\TrilogyEd-Course\Garfunkiel-GeorgiaTech\Lone%20Wolf%20Teacher%20Guide\Axiom%20Tagged%20Files%20Listing\Chrome%20Autofill.csv)” within the Tagged Files Listing folder.

|  |  |  |
| --- | --- | --- |
| Indonesia  jimcloudy1@gmail.com  Bali  fn 5.7 ammo  cloudy-thoughts  9mm ammo | 22030  fn p90  fnp90  Candidasa  mp5  Bali | 9mm sbr  9mm rifle  mp40  rootkey.csv |

(5) An examination of Chrome Autofill records parsed by Magnet Axiom and viewed within Artifact view, revealed 96 Chrome Current Tabs artifacts containing keywords associated with gun control, travel, firearms, public buildings/gatherings and cloud storage associated with the “jcloudy” user profile. For additional details pertaining to timestamps refer to “[Chrome Current Tabs.csv](file:///C:\Users\Thelma%20Looms\Desktop\TrilogyEd-Course\Garfunkiel-GeorgiaTech\Lone%20Wolf%20Teacher%20Guide\Axiom%20Tagged%20Files%20Listing\Chrome%20Current%20Tabs.csv)” within the Tagged Files Listing folder. The following is a representative sample:

* Gun control:
  + gun control great britain - Google Search
  + gun control in indonesia - Google Search
  + PREACH: Gun owner SLAMS leftists over gun violence in an impassioned speech at city council | TheBlaze
  + molon labe - Facebook Search
* Travel:
  + 19 Indonesia Expat Jobs | LinkedIn
  + where the dollar goes farthest vietnam or indonesia - Google Search
  + how to smuggle cash through airport - Google Search
  + hotels in bali - Google Search
* Firearms:
  + keltec 2000 site:gunbroker.com - Google Search
  + Kel-Tec Sub-2000 for Sale - Buy Kel-Tec Sub-2000 Online at GunBroker.com
  + shooting range near me - Google Search
  + Kel-Tec Sub2k Gen2 Glk17 BLACK 9mm $10S&H Sub 2000 : Semi Auto Rifles at GunBroker.com
* Public Buildings/Gatherings:
  + upcoming anti-gun rally near me - Google Search
  + 21030 Whitfield Pl to Dulles International Airport - Google Maps
  + cascades library meeting room b - Google Search
  + reston virginia democratic party building - Google Search
* Cloud Storage:
  + https://s3.console.aws.amazon.com/s3/buckets/cloudy-thoughts/?region=us-east-2&tab=overview
  + will box sync automatically backup desktop - Google Search
  + if i move my desktop to one drive, is it still on my desktop - Google Search
  + how do i set google drive to auto sync - Google Search

(6) An examination of Google Searches records parsed by Magnet Axiom and viewed within Artifact view, revealed 85 Google Search artifacts containing keywords associated with police response times, gun stores, shooting ranges, smuggling cash, public buildings, and cloud storage associated with the “jcloudy” user profile. For additional details pertaining to timestamps refer to “[Google Searches.csv](file:///C:\Users\Thelma%20Looms\Desktop\TrilogyEd-Course\Garfunkiel-GeorgiaTech\Lone%20Wolf%20Teacher%20Guide\Axiom%20Tagged%20Files%20Listing\Google%20Searches.csv)” within the Tagged Files Listing folder. The following is a representative sample:

* can i strap cash to myself and walk through tsa
* Northern Virginia Gun Works
* can i use amazon s3 for free
* Is there a map of gun free zones
* public buildins in reston va
* most beautiful contries with non extradition
* which dc airport has fewest delays
* soviet quote about americans having too many guns
* dulles to bali
* how to use google docs as chat
* Is there a map of gun free zones D.C.
* democratic national headquarters
* get onedrive to automatically sync with folders
* fnp90
* submachine guns
* foldable kel tec
* do the cops track web searches
* police response times by zip code
* sync amazon s3 from desktop?
* concealable tactical rifles
* box sync de3sktop

(7) An examination of Pictures parsed by Magnet Axiom and viewed within Artifact view, revealed 46 Pictures depicting anti-gun control topics, flight itineraries, public buildings, travel routes, and hotels in Indonesia located within multiple directories associated with the “jcloudy” user profile. Pertinent pictures can be viewed with full details within “[Pictures Report.html](file:///C:\Users\Thelma%20Looms\Desktop\TrilogyEd-Course\Garfunkiel-GeorgiaTech\Lone%20Wolf%20Teacher%20Guide\STUDENT%20RELEASABLE%20DOCUMENTS\Axiom%20Example%20Reports\Example%20Axiom%20Pictures%20Report\Pictures%20Report.html)”.

(8) An examination of the “Users/jcloudy/AppData/Local/Packages/Microsoft‌.Office.OneNote” directory using Autopsy revealed seven .bin files containing fragments of a OneNote document referencing willingness to “commit another atrocity”, a “fresh start in Bali”, and “A hundred targets. 2000 bullets. Endless freedom.” For additional details pertaining to timestamps refer to “[Autopsy Report.html](file:///C:\Users\Thelma%20Looms\Desktop\TrilogyEd-Course\Garfunkiel-GeorgiaTech\Lone%20Wolf%20Teacher%20Guide\STUDENT%20RELEASABLE%20DOCUMENTS\Autopsy%20Example%20Report\Autopsy%20Report.html)”. The following [.bin files](file:///C:\Users\Thelma%20Looms\Desktop\TrilogyEd-Course\Garfunkiel-GeorgiaTech\Lone%20Wolf%20Teacher%20Guide\Exported%20Evidence%20Files) may be viewed within a Hexadecimal viewer such as HxD.

* Filename: “00000001.bin” contains:
  + “Cloud Thougts[*sic*]”
  + “Cloud Thoughts”.
* Filename: “00000003.bin” contains:
  + “This might be a better way to keep my thoughts organized, as I can keep a running tab instead of creating new documents every time. I'm still nervous and worried that this wont go as planned, but I'm really looking forward to what could be a fresh start in Bali. This wont be an easy transition, but I hope everyone can understand why I must do this for my country.”
* Filename: “00000016.bin” contains:
  + “Nor can I be sure that everyone wil”
  + “Cloud Thoughts”
  + “This might be a better way to keep my thoughts organized, as I can keep a running tab instead of creating new documents every time. I'm still nervous and worried that this wont go as planned, but I'm really looking forward to what could be a fresh start”
  + “While I'm confident I'm doing the right thing, I cant be sure that it will work. Nor can I be sure that everyone will interpret my actions the way I mean them to be. That s why I left the manifesto and that s why I will continue to type here.”
* Filename: “00000019.bin” contains:
  + “While I'm confident I'm doing the right thing, I cant be sure that it will work. Nor can I be sure that everyone will interpret my actions the way I mean them to be. That s why I left the manifesto and that s why I will continue to type here.”
  + “This might be a better way to keep my thoughts organized, as I can keep a running tab instead of creating new documents every time. I'm still nervous and worried that this wont go as planned, but I'm really looking forward to what could be a fresh start”
* Filename: “0000001A.bin” contains:
  + “Thursday, April 5, 2018”
  + “4:36 AM”
  + “Jim Cloudy”
  + “This might be a better way to keep my thoughts organized, as I can keep a running tab instead of creating new documents every time. I'm still nervous and worried that this wont go as planned, but I'm really looking forward to what could be a fresh start in Bali. This wont be an easy transition, but I hope everyone can understand why I must do this for my country.”
* Filename: “0000001B.bin” contains:
  + “But if I can help delay that atrocity, then I'm willing to commit another atrocity. Operation 2nd Hand Smoke is a go on Saturday. A hundred targets. 2000 bullets. Endless freedom.”
  + “Taking away guns limits our ability to protect ourselves from criminals. But it also (surprise) limits our ability to protect ourselves from an abusive government. Sure, at this moment there isn't a big problem with the government oppressing us (just little ones), but that doesn t mean there won't be a problem in 100 years. Laws last until they are no longer needed. If it ever passed, a gun ban would never be repealed, for the same reason it passed. Guns are easy to point to, and any politician who tried to rally support to repeal would be looked at as though he didn t care about our safety. The left”
  + “While I'm confident I'm doing the right thing, I cant be sure that it will work. Nor can I be sure that everyone will interpret my actions the way I mean them to be. That s why I left the manifesto and that s why I will continue to type here.”
  + “I've been increasingly caught off guard by the level of deception being implemented by gun control Nazis. The use of crisis actors is certainly shocking. The use of child protestors/crisis actors is shockingly brilliant. They can say whatever they want, but if we rebut their lies, its equated to child abuse. How dare you attack this teenager who is sharing our propaganda!”
  + “Reading an article now about a bomb that blew up at Sam's club. https://www.theblaze.com/news/2018/04/05/explosive-device-detonated-in-a-sams-club-second-device-found-in-suspects-car”
  + “Bombs are illegal. You cant buy them at the store. Killers are going to kill regardless of the law. Cain killed able with a rock. Regardless of our laws criminals will break them to achieve their goals.”
  + “The gun nazis will only get stronger, so it may be that the 2nd amendment will die regardless.”
  + “https://www.theblaze.com/video/preach-gun-owner-slams-leftists-over-gun-violence-in-impassioned-speech-at-city-council Wow! That s exactly it. If we give up our guns, the gangsters won't. Its illegal for the gangs to have guns now. But the cops don t have the ability to take them. But they can take the law abiding citizens' guns, because they will abide by the law. They will do what the law says. And then the gangs will take over. Who's going to protect us then. Cant protect ourselves, the police are already overworked, and oh yeah, they are bad guys too apparently. They cant even protect themselves without being sued or retaliated against. So how are they going to prte”
* Filename: “0000001C.bin” contains:
  + “Things are looking up. I've got my bags mostly packed already. Gave the account information to my brother, who at some point will probably read this. Hello. And it looks like the weather is clearing up for Saturday, so no snow delays! Maybe this is a sign from God. I am doing what I need to for this country. With God on my side, I can't fail.”

(9) An examination of the “Users/jcloudy/AppData/Local/ Google/Chrome/User Data/Default/IndexedDB/https\_docs.google.com\_0.indexeddb.leveldb/” directory using Autopsy revealed a database file containing Google Docs data. The Google Doc appears have been used as a chat forum, wherein multiple users can type simultaneously. For additional details pertaining to timestamps refer to “[Autopsy Report.html](file:///C:\Users\Thelma%20Looms\Desktop\TrilogyEd-Course\Garfunkiel-GeorgiaTech\Lone%20Wolf%20Teacher%20Guide\STUDENT%20RELEASABLE%20DOCUMENTS\Autopsy%20Example%20Report\Autopsy%20Report.html)”. The following file should be viewed within Autopsy’s Indexed Text viewer.

* Filename: “000044.ldb” contains:
  + “Brother Chat”
  + “Hey, Paul its me. Just thought this would be easier and safer honestly.”
  + “WTF, Jim. This is wierd. What are you researching that would bring th feds to your door? Why would anyone care what you research, there are thousands of people researching guns and gun control now days. Why would you stand out?”
  + “m not saying I would stand out, I m just conderned. I just read somewhere about a family who s mom researched a crock pot and the dad researched a backpack and boom...feds at the door. So obviously they are watching everyone s history. I dont want to get visited by the cops. They want find any terrorism stuff, but I have a little garden they might be interested in once they arrive.”
  + “So you are worried they will come by just to check and find a real reason to get you...ok”
  + “Exactly, man. I just think that chatting on here will be simpler anyway. I promise not to get mad...lol.”

(10) An examination of the Ex 1 revealed multiple cloud accounts and upload/sync applications.

* Email addresses:
  + Jimcloudy1@gmail.com
  + jimcloudy@outlook.com
* Amazon Web Services (AWS) Simple Storage Service (S3)
  + Filename: “[rootkey.csv](file:///C:\Users\Thelma%20Looms\Desktop\TrilogyEd-Course\Garfunkiel-GeorgiaTech\Lone%20Wolf%20Teacher%20Guide\Exported%20Evidence%20Files\rootkey.csv)” contains public/private keys for AWS. For additional details refer to “[AWS Keys.csv](file:///C:\Users\Thelma%20Looms\Desktop\TrilogyEd-Course\Garfunkiel-GeorgiaTech\Lone%20Wolf%20Teacher%20Guide\Axiom%20Tagged%20Files%20Listing\AWS%20Keys.csv)”.
    - AWSAccessKeyId=AKIAJQCL74OG6U6JRXKQ
    - AWSSecretKey=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

|  |  |
| --- | --- |
| Account Web Address | Username |
| Microsoft | jimcloudy@outlook.com |
| OneDrive | jimcloudy@outlook.com |
| Google | jimcloudy1@gmail.com |
| Dropbox | jimcloudy1@gmail.com |
| Twitter | jimcloudy1@gmail.com |
| Box | jimcloudy1@gmail.com |
| Amazon Web Services | jimcloudy1@gmail.com |
| Facebook | jimcloudy1@gmail.com |

4. **CONCLUSION.**

The examination of Ex 1 disclosed evidence to show the user “jcloudy” conducted multiple internet searches pertaining to the procurement of weapons and ammunition, locations to attack, and evading capture and extradition. User “jcloudy” authored documents which appear to indicate the user was preparing to conduct an attack during the town hall meeting located at the Cascades Library on Saturday, 7 April between 12:30PM and 2:00PM local time, then fly from Dulles International Airport to Denpasar Airport near Bali, Indonesia.

User “jcloudy” has access to multiple cloud applications and services which can be used to communicate or store data. Only partial content could be recovered from the OneNote file “Jim’s Notebook”. OneNote files are automatically synced to their associated OneDrive accounts and, unless deleted by the user, could be recovered directly from the OneDrive account. Dropbox, Twitter, Box, Amazon Web Services, and Facebook send verification emails and account updates to the email address associated with their accounts; therefore, it is likely Gmail account jimcloudy1@gmail.com will contain information pertaining to these accounts. These emails may assist in determining when the accounts were created.

Examination revealed evidence indicating user “jcloudy” used OneDrive, Google Drive, Dropbox, Box, and Amazon S3 to backup files. These files will persist until deleted by the user and can be obtained through a Search Warrant. Amazon Web Services accounts require a credit card for signup. Obtaining this information may assist in determining the owner of the Amazon S3 bucket.

|  |  |
| --- | --- |
| Encl.  Findings Disk. | ///ORIGINAL SIGNED///  IAM THE FORENSICATOR  Senior Digital Forensic Examiner |