

**INVESTIGATIVE REPORT  
VERMONT STATE POLICE**

**CASE NUMBER:** 18B302863

**OFFICER:** Detective Sergeant Alberico

**INCIDENT/STATUTE VIOLATION:**

**DATE/TIME OF INCIDENT:**

**LOCATION OF INCIDENT:** [REDACTED] Bennington, VT

**CASE OFFICER:** Detective Sergeant Henry Alberico

**SUSPECT/ACCUSED:**

**VICTIM(S):** Ruqaiyah Morris [REDACTED]  
[REDACTED]  
Bennington, VT

James Lawton [REDACTED]  
[REDACTED]  
Bennington, VT

**LIST OF POLICE WITNESSES:**

Detective Sergeant Henry Alberico (Vermont State Police)  
Detective Trooper Eric Jollymore (Vermont State Police)  
Chief Paul Doucette (Bennington Police Department)  
Officer Michael Sharshon (Bennington Police Department)

**WITNESSES:**

[REDACTED]

[REDACTED]

[REDACTED]

**LIST OF EXHIBITS:**

(2) Investigative Action Reports

**NARRATIVE:**

On August 29, 2018, I was assigned a "special investigation" and was provided with documents from an investigation that was conducted by the Bennington Police Department. It should be noted that all of Bennington Police Department's documents will be included with this case for review.

I learned that Ruqaiyah Morris [REDACTED] and her husband James Lawton [REDACTED] had filed a complaint with the Bennington Police Department on July 27, 2018 (Bennington PD Case #18BN05584). Lawton had spoke with Officer Michael Sharshon (Bennington Police Department) in regards to issues he and his wife (Morris) were having with someone he referred to as a "local neo-nazi." The individual was identified as Max Misch [REDACTED] and was said to be causing issues for Morris and Lawton online.

Through further discussion Officer Sharshon learned that Mish had been targeting Morris on social media (Facebook & Twitter) and making unpleasant comments. Print outs of the comments being referred to by Lawton are included with this case, however, the conversations do not appear to be in their entirety.

Lawton then stated that he had signed onto his computer and discovered that the "sign on name" had been changed. Lawton explained that this sign on name typically shows "James Lawton" however, when he signed on he found it to say "dead dead."

During Lawton's conversation with Officer Sharshon, he explained that Morris was currently in legislative session (Morris is a VT representative) and she had been speaking with the Vermont State Police (VSP). Lawton informed Sharshon that he believed VSP would take the computer and asked if he should bring it to the Bennington Police Department and Sharshon informed him, "no." Officer Sharshon directed Lawton to speak with Morris and inquire about what VSP wanted done with the computer.

On July 30, 2018, Officer Sharshon learned that Lawton had brought his computer to the Bennington Police Department. Officer Sharshon contacted Detective Trooper Eric Jollymore (VSP TIU) and documented in his report that "...that situation that Lawton encounter is possible, however, it would require whoever did it to have an advanced degree of technical knowledge of computers. It was determined that the computers would not be forensically analyzed."

On August 8, 2018 Matthew Raymond (VT Internet Crimes Taskforce Commander) entered a supplemental report into Officer Sharshon's report (18BN05584), which in part stated, "This case was brought to my attention as the Commander of the Vermont Internet Crimes Against Children Taskforce (VT-ICAC). There was an impression that VT-ICAC recommended that no computer exam be conducted. I am writing this report to correct that impression. Trooper Jollymore advised Officer Sharshon that VT-ICAC would conduct a computer exam if requested and that it was possible to obtain evidence from such a computer exam to advance the investigation. VT-ICAC is ready to accept the computer for examination should one be requested."

September 6, 2018, I was scheduled for an interview with Morris, Lawton, and their attorney Robert Appel at the Vermont State Police barracks in Shaftsbury. While Lawton and Morris awaited the arrival of Appel, Lawton complained of discomfort in his chest. Morris and Lawton explained that he was scheduled for "bypass surgery" the following week. For precautionary reasons, Bennington Rescue was contacted. Upon their arrival members of Bennington Rescue assessed Lawton and subsequently transported him to the medical center in Bennington, VT. The interview was cancelled and later rescheduled for September 19, 2018.

On September 19, 2018, while en route to the Morris and Lawton residence, I was notified that due to ongoing health issues with Lawton, they would need to cancel the appointment. Morris was requested to photograph both the front and rear of her in home router and forward the same photographs to VSP TIU. Morris complied with the request. Morris and Lawton agreed to meet with me at the Shaftsbury Barracks on October 3, 2018 to discuss this case.

On October 3, 2018, Detective Eric Jollymore and I interviewed Morris and Lawton at the Vermont State Police barracks in Shaftsbury, VT. Attorney Appel was present during both interviews. The interviews were audio/video recorded and copies of the recordings are on file with this case.

At approximately 1007 hours, we met with James Lawton and spoke in detail about the complaint he filed on July 27, 2018.

I explained to Lawton that I knew there had been many different complaints and incidents that he had been a part of over the last two years. I further explained that my primary focus was going to be the most recent complaint that he had made, in regards to the "Dead Dead" screen name that appeared on his computer.

Lawton explained that on July 27, 2018 he had flipped open his computer screen and saw that his screen name had been changed to "Dead Dead." Lawton had told Morris that he had seen something weird on his screen. Lawton said that he had told Morris prior to her leaving to Montpelier. He felt that his computer had been hacked into, because the night before he had been doing research on "Neo Nazi" groups that were connected to "Max Misch." Lawton said he has a fake Instagram account, however, he does not have one for

Facebook. Lawton felt by looking at the "Neo Nazi" groups from his personal Facebook account, the groups were able to detect his inquires and then hacked into his account.

Lawton opened his computer a second time during the morning hours on July 27, 2018 and again observed "Dead Dead" as his log in name. He photographed the screen name and forwarded it Morris. Morris then went directly to the Capitol Police and reported it. Lawton then received a message from Morris advising the "IT department form the State House" said to turn off the computer, unplug it, shut off the Wi-Fi, and remove the battery.

Lawton explained that he became very concerned after the IT tech at the State House had expressed a theory that someone had to be within close proximity of their (Lawton/Morris) residence in order to utilize their Wi-Fi and effect the login name change. Lawton further explained that he would not have been concerned for his family's safety if this had been done by someone out of state, but it was rather unsettling to think someone was close enough to their home to do such a thing.

Lawton said that he and Morris were directed by the Attorney General's office to bring the computers to the Bennington Police Department. Morris called Bennington Police Chief Doucette and shared the above information. Lawton and Morris then brought their computers to the Bennington Police Department on Saturday July 28, 2018 and turned them over as evidence. Bennington Police Officer Sharshon handled the complaint filed on July 27, 2018 by Lawton and the details are reflected in Bennington Police Department case # 18BN05584. A copy of the report(s) associated with that case are attached and incorporated for further review.

Lawton's computer was subsequently forwarded to the Vermont State Police Technology Investigation Unit (TIU) for a forensic analysis. As a result Detective Trooper Eric Jollymore had completed a report of the analysis, which is attached to this case and available for further review.

In Detective Jollymore's report it indicated that there had been other log in names utilized, which included [REDACTED] "Chicken Nugget," "James Lawton," and "Dead Dead." Lawton explained that he had purchased his HP computer from the Facebook Market Place from a girl named [REDACTED]. He explained that the screen name containing [REDACTED] was hers. He acknowledged seeing "Chicken Nugget" at some point, however, it was not a login that he had created. He did state that when creating a login, he used "James Lawton." He reiterated that the log in name "Dead Dead" that was displayed with (Lawton's) picture was not a login that he created.

At approximately 1223 hours, Detective Eric Jollymore and I then met with Ruqaiyah Morris and spoke of the incident surrounding the July 27, 2018 complaint Lawton had reported to the Bennington Police Department.

Morris explained that on July 27, 2018, she had an early morning meeting in Montpelier. Morris said that prior to her leaving for her meeting, Lawton had told her that the screen

on his computer looked "weird." Lawton explained that there was a "weird thing" on his screen. Morris left and drove to Montpelier. She called Lawton once she arrived in Montpelier and informed him that she had arrived safely. While on the phone with Lawton, he told Morris that "it came back up." Lawton told Morris that their son, [REDACTED] had seen it. Lawton's screen name had been changed to "Dead Dead."

Lawton took a picture of the screen and sent it to Morris. Morris then forwarded the same picture to a friend of hers who works in "IT" in the Seattle Washington area. The friend told Morris "this is bad, it looks like doxing." Morris was told to make a report to law enforcement.

Morris said she then contacted Legislative Council and the State House IT department. Morris said that Legislative Council then contacted the Capitol Police and informed them of the situation. Morris was called later in the day by an Officer from the Capital Police and Kevin Moore from "IT." Morris said she showed both of them the screen shot of Lawton's computer screen. The "IT" representative directed Morris to power down the computer, pull the battery, and get them to law enforcement. They informed Morris that her computer was "seriously compromised."

Morris explained that she was very shaken and called her friend, who is a Deputy States Attorney from Washington County, Ashley Hill. Hill directed Morris to the Vermont State Police and told her to turn her computers over. Morris said she went to the barracks in Washington County (later advised it was Middlesex barracks) and informed a Trooper of her complaint. Morris added that a formal report was not taken. Morris said she was provided the number for "PAVE." The trooper explained the process to Morris about applying for an emergency "RFA" (relief from abuse order). Morris explained that she was very familiar with the process and knew how an emergency RFA works.

Morris then called Bennington Police Chief Paul Doucette and left him a voicemail, detailing the agencies she had contact with and that her husband would be bringing the computers to the Bennington Police for examination. This interaction is documented in Bennington Police Department's case # 18BN05584 and a copy of the report is attached to this case.

On October 10, 2018, I met with [REDACTED]. While meeting with [REDACTED] she acknowledged selling a laptop HP computer to Lawton earlier in the year. I asked [REDACTED] if she remembered any of the user names that were used on the computer. Wright stated she had an email setup, in order for her ten year old son [REDACTED] to use his Xbox. [REDACTED] also acknowledged having used "chicken nugget" previously as well. I asked [REDACTED] specifically if she had ever used the name "dead dead" and she said she had not. She informed me that [REDACTED] plays a lot of "shooting games" on Xbox and that sounded like a name he could have possibly used. [REDACTED] fiancée, [REDACTED] was present during the interview and powered on [REDACTED] Xbox while I was speaking with [REDACTED]. [REDACTED] returned and informed me that the name "James Lawton" had appeared on the screen, when powering on the Xbox. I went into [REDACTED] bedroom and observed

three names flashing on the screen, "James Lawton," "[REDACTED]" and "DxY kitten." [REDACTED] explained that the "[REDACTED]" is the email account that she set up specifically for [REDACTED]. [REDACTED] did not know why "James Lawton" was appearing on the screen and added that "DxY kitten" is [REDACTED] Xbox name. At the time I met with [REDACTED], [REDACTED] was in school and it was decided that I would return later in the afternoon, in order to speak to him about the names appearing on his Xbox screen.

I returned later in the afternoon and met with [REDACTED], in the presence of his mother ([REDACTED]) and her fiancée ([REDACTED]). [REDACTED] explained that his Xbox user name is "DxY kitten" and he can set up secondary names. [REDACTED] said that he saw the name "James Lawton" appear on his screen one day, so he changed it to "dead dead." [REDACTED] said that he and his sister have an ongoing joke, where they tell each other they are "dead inside." [REDACTED] said the "dead dead" name had been deleted by someone and switched back to "James Lawton." [REDACTED] said he never changed the name again and left it as "James Lawton." While discussing these changes, [REDACTED] suggested that "James" could change his account. [REDACTED] told [REDACTED] that she would just start a new account for [REDACTED] and he was adamant that she not change his account and that James needed to change his. Through further discussion we learned that [REDACTED] was afraid to lose everything connected to his Xbox account and added that was why he didn't tell anyone about the name "James Lawton" being on the screen. The interview with [REDACTED] was recorded and a copy of the recording has been filed with this case.

#### SUMMARY:

On July 27, 2018, James Lawton filed a complaint with the Bennington Police Department, reporting that he had received a death threat on his laptop computer. During the investigation it was learned that Lawton had purchased a HP laptop from [REDACTED]. [REDACTED] Lawton had created a login name "James Lawton" and utilized that screen name while using the laptop computer. When using the laptop computer during the morning hours of July 27, 2018, Lawton observed the login name "Dead Dead." Lawton informed his wife, Ruqaiyah Morris, of his findings. The name appeared later in the day as well and he again informed Morris of his findings. Morris, being a State of Vermont Representative, reported it to members of Legislature, Legislative IT department, and the Capitol Police. The laptop was subsequently turned over to the Bennington Police Department as evidence. The same computer was forwarded to the Vermont State Police Technology Investigation Unit (VSP TIU) for a forensic analysis.

The HP laptop belonging to James Lawton was analyzed by members of VSP TIU and Detective Jollymore completed a 20 page analysis report, which is attached for further review.

On October 3, 2018, I met with Lawton and he in fact acknowledged purchasing a HP laptop computer from Facebook Market Place from a female named [REDACTED]. Lawton explained that he tried to reset the computer to the best of his ability. Lawton said

he did not send the laptop to a professional to have it "cleaned" or reset to original factory condition. Lawton said that he had created the Microsoft Live login screen name of "James Lawton." On July 27, 2018, Lawton first noticed his screen name had been changed to "Dead Dead." Lawton informed his wife of his findings and later reported it to the Bennington Police Department. Lawton advised that he had changed the screen name back to "James Lawton."

On October 10, 2018, I met with [REDACTED] and confirmed that she had sold a HP laptop computer to James Lawton earlier in the year. [REDACTED] also advised that she had a Microsoft Live account ([REDACTED]), so her ten year old son, [REDACTED] could use his Xbox. While at [REDACTED] residence, her son's Xbox was powered on and I observed the screennames, "James Lawton," "DxY kitten," and [REDACTED]. I also spoke with [REDACTED] and he acknowledged having an Xbox and that his username is "DxY kitten." [REDACTED] also added that he had seen the name "James Lawton" appear on his Xbox screen. [REDACTED] changed the name "James Lawton" to "Dead Dead." [REDACTED] explained that he and his sister always joke about being "dead inside" and that is what he was referencing when creating the screen name "Dead Dead." [REDACTED] said that the name "Dead Dead" had been changed back to "James Lawton." [REDACTED] never reported these events to his parents and I learned that he was fearful of losing all of his materials saved to the Xbox.

In conclusion, both James Lawton and [REDACTED] had admittedly utilized the same Microsoft Live accounts for their own personal use. Neither Lawton nor [REDACTED] believed anyone had the ability to make changes to their specific account. Both [REDACTED] and Lawton implemented changes to their own accounts, however, inadvertently imposed changes to the other persons. There is no evidence indicating either Lawton or [REDACTED] had knowledge of the connection between their accounts. Furthermore, there is no evidence that either change was made with malicious or threatening intent, which would constitute criminal charges.

A complete copy of this case will be forwarded to the Attorney General's office for their review and recommendation.



**VERMONT STATE POLICE**  
**Bureau of Criminal Investigation**  
**Investigative Actions Narrative**

Investigative actions taken on 09/06/18 by Det. Sgt. Henry Alberico

Case#: 18B302863

Narrative:

On September 6, 2018, I drove to the Vermont State Police barracks in Shaftsbury, VT for the purpose of conducting an interview with Ruqaiyah Morris [REDACTED] and her husband James Lawton [REDACTED] in the presence of their attorney Robert Appel. Morris and Lawton arrived at the Shaftsbury barracks prior to Appel. While waiting in the lobby, Lawton complained of discomfort in his chest and requested to lay down. Morris and Lawton explained that Lawton was scheduled for "bypass surgery" the following week. Lawton and Morris were informed that Bennington Rescue was going to be contacted and requested to respond to the barracks for precautionary reasons, in order to assure Lawton was medically OK.

Bennington Rescue responded to the barracks and subsequently transported Lawton along with Morris to the Medical Center in Bennington.

Appel arrived at the Shaftsbury barracks shortly after Bennington Rescue departed with Lawton and Morris. Appel agreed that the interview would be rescheduled for a later date, once Lawton was medically cleared to participate.

End of Report.





**VERMONT STATE POLICE**  
**Bureau of Criminal Investigation**  
**Investigative Actions Narrative**

Investigative actions taken on 09/19/18 by Det. Sgt. Henry Alberico

Case#: 18B302863

Narrative:

On September 19, 2018, arraignments had been made for myself and an investigator from the VSP TIU to meet with Ruqaiyah Morris [REDACTED] and her husband James Lawton [REDACTED] at their residence located at [REDACTED] in Bennington, VT. The purpose of this meeting was for the TIU investigator to examine and evaluate the home router belonging to Morris and Lawton. Prior to the scheduled meeting Morris canceled, due to issues with her husband's (Lawton) health.

Morris was requested to photograph the front and back side of the router inside of her residence. Morris completed the photographs and forwarded them to the VSP TIU as requested.

Morris agreed to reschedule the interview for October 3, 2018 at the Shaftsbury barracks at 10am.

End of Report.



***VERMONT STATE POLICE***  
***Bureau of Criminal Investigation***  
**Investigative Actions Narrative**

Investigative actions taken on 10/03/18 by Det. Sgt. Henry Alberico

Case#: 18B302863

Narrative:

On October 3, 2018, Detective Trooper Eric Jollymore and I conducted recorded interviews of James Lawton and Ruqaiyah Morris at the Shaftsbury barracks. Lawton and Morris' attorney, Robert Appel was present for both interview. Reports for both interviews have been authored and attached to the case.

Copies of the audio recordings have also been filed with this case.

End of Report.



**VERMONT STATE POLICE**  
**Bureau of Criminal Investigation**  
**Investigative Actions Narrative**

Investigative actions taken on 10/10/18 by Det. Sgt. Henry Alberico

Case#: 18B302863

Narrative:

On October 10, 2018, at approximately 1248 hours, I met with [REDACTED] [REDACTED] for the purpose of conducting an interview in regards to a computer she sold to James Lawton earlier in the year. This interview was recorded and a file of the entire interview is on file and a "Persons Interviewed" report has been compiled, detailing the interview in its entirety.

A Copy of the audio recording has been filed with this case.

End of Report.



**VERMONT STATE POLICE**  
**Bureau of Criminal Investigation**  
**Investigative Actions Narrative**

Investigative actions taken on October 3, 2018 by Det. Sgt. Henry Alberico & Detective Trooper Eric Jollymore

Case#: 18B402863

Officer: Det. Sgt. Henry Alberico

Person Interviewed:

James Lawton [REDACTED]

Bennington, VT  
[REDACTED]

Exhibits: (1) CD of Audio recorded statement

Narrative:

On October 3, 2018 at approximately 1007 hours, Detective Eric Jollymore and I met with James Lawton [REDACTED], along with his Attorney Robert Appel at the Vermont State Police barracks in Shaftsbury. The purpose of the interview was to investigate a threatening complaint that had been filed by Lawton and his wife Ruqaiyah Morris [REDACTED].

I explained to Lawton that I knew there had been many different complaints and incidents that he had been a part of over the last two years. I further explained that my primary focus was going to be the most recent complaint that he had made, in regards to the "Dead Dead" screen name that appeared on his computer.

Lawton explained that on July 27, 2018 he had flipped open his computer screen and saw that his screen name had been changed to "Dead Dead." Lawton had told Morris that he had seen something weird on his screen. Lawton told this to Morris prior to her leaving to Montpelier. He felt that his computer had been hacked into, because the night before he had been doing research on "Neo Nazi" groups that were connected to "Max Misch." Lawton said he has a fake Instagram account, however, he does not have one for Facebook. Lawton felt by looking at the "Neo Nazi" groups from his personal Facebook account, the groups were able to detect his inquires and then hacked into his account.

Lawton opened his computer a second time during the morning hours on July 27, 2018 and again observed "Dead Dead" as his log in name. He photographed the screen name and forwarded it Morris. Morris then went directly to the Capitol Police and reported it. Lawton then received a

message from Morris advising the "IT department from the State House" said to turn off the computer, unplug it, shut off the Wi-Fi, and remove the battery.

Lawton explained that he became very concerned after the IT tech at the State House had expressed a theory that someone had to be within close proximity of their (Lawton/Morris) residence in order to utilize their Wi-Fi and effect the login name change. Lawton further explained that he would not have been concerned for his family's safety if this had been done by someone out of state, but it was rather unsettling to think someone was close enough to their home to do such a thing.

Lawton said that he and Morris were directed by the Attorney General's office to bring the computers to the Bennington Police Department. Morris called Bennington Police Chief Doucette and shared the above information. Lawton and Morris then brought their computers to the Bennington Police Department on Saturday July 28, 2018 and turned them over as evidence. Bennington Police Officer Sharshon handled the complaint filed on July 27, 2018 by Lawton and the details are reflected in Bennington Police Department case # 18BN05584. A copy of the report(s) associated with that case are attached to and incorporated for further review.

Lawton's computer was subsequently forwarded to the Vermont State Police Technology Investigation Unit (TIU) for a forensic analysis. As a result Detective Trooper Eric Jollymore had completed a report of the analysis, which is attached to this case and available for further review.

In Detective Jollymore's report it indicated that there had been other log in names utilized, which included "██████" "Chicken Nugget," "James Lawton," and "Dead Dead." Lawton explained that he had purchased his computer from Facebook market place from a girl named ██████. He detailed that the screen name connected ██████ was hers. He acknowledged seeing "Chicken Nugget" at some point, however, it was not a login that he had created. He did state that when creating a login, he used "James Lawton." He reiterated that the log in name "Dead Dead" that was displayed with (Lawton's) picture was not a login that he created.

The interview with Lawton was recorded and this a synopsis of the interview. A copy of the entire interview is on file with the case.



**VERMONT STATE POLICE**  
**Bureau of Criminal Investigation**  
**Investigative Actions Narrative**

Investigative actions taken on October 3, 2018 by Det. Sgt. Henry Alberico & Detective Trooper Eric Jollymore

Case#: 18B402863

Officer: Det. Sgt. Henry Alberico

Person Interviewed:

Ruqaiyah Morris [REDACTED]

Bennington, VT  
[REDACTED]

Exhibits: (1) CD of Audio recorded statement

Narrative:

On October 3, 2018 at approximately 1223 hours, Detective Eric Jollymore and I met with Ruqaiyah Morris [REDACTED], along with her Attorney Robert Appel at the Vermont State Police barracks in Shaftsbury. The purpose of the interview was to continue a threatening complaint that had been filed by Morris and her husband James Lawton [REDACTED].

I explained to Morris that I knew there had been "a lot going on" over the past few years, however, my primary focus was on the most recent complaint that she and Lawton had made. The complaint was in regards to a potential threat that was received over Lawton's computer.

On one particular Friday morning, Morris explained that she had an early morning meeting in Montpelier. Morris said that prior to her leaving for her meeting, Lawton had told her that the screen on his computer looked "weird." Lawton explained that there was a "weird thing" on his screen. Morris left and drove to Montpelier. She called Lawton once she arrived in Montpelier and informed him that she had arrived safely. While on the phone with Lawton, he told Morris that "it came back up." Lawton told Morris that their son, [REDACTED] had seen it. Lawton's screen name had been changed to "Dead Dead."

Lawton took a picture of the screen and sent it to Morris. Morris then forwarded the same picture to a friend of hers who works in "IT" in the Seattle Washington area. The friend told Morris "this is bad, it looks like doxing." Morris was told to make a report to Law Enforcement.

Morris said she then contacted Legislative Council and the State House IT department. Morris said that Legislative Council then contact Capitol Police and informed them of the situation.

Morris was called later in the day by an Officer from the Capital Police and Kevin Moore from "IT." Morris said she showed both of them the screen shot of Lawton's computer screen. The "IT" representative directed Morris to power down the computer, pull the battery, and get them to Law Enforcement. They informed Morris that her computer was "seriously compromised."

Morris explained that she was very shaken and called her friend, who is a Deputy States Attorney from Washington County, Ashley Hill. Hill directed Morris to the Vermont State Police and told her to turn her computers over. Morris said she went to the barracks in Washington County (later advised it was Middlesex barracks) and informed a Trooper of her complaint. Morris added that a formal report was not taken. Morris said she was provided the number for "PAVE." The trooper explained the process to Morris about applying for an emergency "RFA" (relief from abuse order). Morris explained that she was very familiar with the process and knew how an emergency RFA works.

Morris then called Bennington Police Chief Paul Doucette and left him a voicemail, detailing the agencies she had contact with and that her husband would be bringing the computers to the Bennington Police for examination. This interaction is documented in Bennington Police Department's case # 18BN05584 and a copy of the report is attached to this case.

I had asked Morris if she had had access to Lawton's laptop and she advised that she never uses his computer, due to the fact that she has her own. Morris also indicated that she had not used the Lawton's computer and did not change his username to "Dead Dead."

The interview with Morris was recorded and this a synopsis of the interview. A copy of the entire interview is on file with the case for review.



**VERMONT STATE POLICE**  
**Bureau of Criminal Investigation**  
**Investigative Actions Narrative**

Investigative actions taken on October 10, 2018 by Det. Sgt. Henry Alberico

Case#: 18B302863

Officer: Det. Sgt. Henry Alberico

Person Interviewed:

Exhibits: (1) CD of Audio recorded statement

Narrative:

On October 10, 2018 at approximately 1248 hours, I met with [REDACTED] at her residence, located at [REDACTED]. The purpose of the interview was to continue an investigation into a threatening complaint that had been filed by Ruqaiyah Morris [REDACTED] and her husband James Lawton [REDACTED].

I explained to [REDACTED] that I wanted to speak about a computer that she had sold earlier in the year. [REDACTED] stated that she had sold two computers, one that had belonged to her and one that had belonged to her mother. [REDACTED] added that her computer was sold to a man that lived on [REDACTED] in Bennington and the other computer was sold to someone that worked at the Bank of Bennington in Bennington, VT. I told [REDACTED] the computer that I was interested in talking about was the one she sold to the person on [REDACTED]. [REDACTED] added that specific computer had been hers. I further told [REDACTED] that a possible threat had been received on the computer she had sold, however, Law Enforcement was trying to rule out all user names/log ins that had been utilized on the computer.

[REDACTED] explained that there were multiple log-in's that could have been used on that computer. Some of the log-in's that she provided, included "Chicken Nugget, [REDACTED], [REDACTED] [REDACTED]." I specifically asked [REDACTED] if "Dead Dead" would have been a possible username and she informed me that her ten year old son [REDACTED] plays video games on the Xbox and plays games like "Call of Duty, the shooting kind of dying games." [REDACTED] added that she felt that the "Dead Dead" was certainly something that her son [REDACTED] could have created and they were somehow linked on the Xbox and lap top she had sold to Lawton.



While speaking with [REDACTED], her fiancée, [REDACTED], had turned on [REDACTED] Xbox and advised that the name "James Lawton" immediately appeared on the screen. I looked at the screen and confirmed that the name "James Lawton" was in fact linked to the Xbox account that was used by [REDACTED]. "James Lawton" was also showing a name of "DxY kitten." I photographed (11 photographs) the screen which was displaying "James Lawton" and [REDACTED]. [REDACTED] explained that the "[REDACTED]" [REDACTED] is the account that her son [REDACTED] uses for the Xbox account.

The interview with [REDACTED] was recorded and this a synopsis of the interview. A copy of the entire interview is on file with the case.



**VERMONT STATE POLICE**  
**Bureau of Criminal Investigation**  
**Investigative Actions Narrative**

Investigative actions taken on October 10, 2018 by Det. Sgt. Henry Alberico

Case#: 18B302863

Officer: Det. Sgt. Henry Alberico

Person Interviewed:



Exhibits: (1) CD of Audio recorded statement

Narrative:

On October 10, 2018 at approximately 1740 hours, I met with [REDACTED] and his mother, [REDACTED] at their residence, located at [REDACTED]. The purpose of the interview was to continue an investigation into a threatening complaint that had been filed by Ruqaiyah Morris [REDACTED] and her husband James Lawton [REDACTED].

I had met with [REDACTED] earlier in the day and discussed the sale of a lap top computer, which she ultimately had sold to James Lawton. While meeting with [REDACTED] she had mentioned that she had an "outlook" email account that she had set up so her son, [REDACTED], could use it on his Xbox. [REDACTED] fiancée, [REDACTED], had turned the Xbox on while I was at the residence and discovered that the name "James Lawton" appeared on the screen.

While meeting with [REDACTED], I explained to him that he was not in any type of trouble and that I had a few questions surrounding his Xbox account. I asked [REDACTED] about names that he uses on Xbox and he explained that his actual screenname his "DxY kitten." [REDACTED] further explained to me that Xbox has a system that allows you to actually enter your "real life name." [REDACTED] explained that he had made his name "Dead Dead." [REDACTED] said that he and his sister have a running joke where he tells her "Hey, I am dead inside." [REDACTED] said he did not use any other names and thought he had used "Dead Dead" for a month or two time period. [REDACTED] said the reason he stopped using "Dead Dead" was because it had been changed to James Lawton. [REDACTED] said he initially used the name "[REDACTED]" and it then changed to "James Lawton" [REDACTED] said he did not know who that was and then [REDACTED] changed it to "Dead Dead." [REDACTED] said that the secondary name on his account is currently James Lawton.

While speaking with [REDACTED] he stated that James could create a new Microsoft account and [REDACTED] replied that she could create a new one for [REDACTED]. [REDACTED] was very adamant that his account could not be closed, as he would lose all of his Xbox information.

The interview with [REDACTED] was recorded and this a synopsis of the interview. A copy of the entire interview is on file with the case.

18BN05584

Vermont State Police Technology Investigation Unit  
Analysis Report

Case Number: 18BN05584  
Suspect: Unknown

---



Examiner: Det. Tpr. Eric Jollymore  
Computer Crimes

**Case Information:**

**Department:** Bennington Police Department / Vermont State Police – New Haven

**Incident Number:** 18BN05584\* & 18B302863

*This analysis was started under the case 18BN05584. For organization purposes all tool reports and analysis work remained organized as 18BN05584.*

**Investigator:** Det. Sgt. Henry Alberico

**Suspect:** Unknown

**Date of Incident:** 7.27.2018

**Location:** [REDACTED] Bennington, Vermont

**Nature of Incident:** Threatening

**Associated Materials:**

- XWF Reports
  - 18BN05584 - Item 2 Event Log Issue List.xlsx
- XWF Processing Options Reports
  - 18BN05584 - Item 2 Extensive Data Carving Processing Options.txt
  - 18BN05584 - Item 2 Extensive Data Carving Selections.txt
  - 18BN05584 - XWF Initial Processing Options.txt (Both Items)
  - 18BN05584 - XWF VSS Processing Options.txt (Item 2)
- RegRipper Reports
  - 18BN05584 - Item 2 SAM Registry RegRipper Output.txt
  - 18BN05584 - Item 2 [REDACTED] Registry RegRipper Output.txt
- EnCase Reports
  - 18BN05584 - EnCase - Initial Processing Options.rtf
- IEF Reports
  - 18BN05584 - IEF Case Information and Processing Options.txt
  - CSV Export 2018-09-12\_13-55-47 (5 CSV reports)
    - Chrome FavIcons.csv
    - Chrome Web History.csv
    - Chrome Web Visits.csv
    - Chrome-360 Safe Browser-Opera Carved Web History.csv
    - User Accounts.csv
- Excel Spreadsheets
  - 18BN05584 - Test VM Timeline notes.xlsx
- Virtual Machines
  - Windows 10 x64 - TEST VM 18BN05584.vmwarevm
- Virtual Machine Test Materials
  - 18BN05584 – VM Test Saved Events (6 Files)
- Preservation Materials

Commented [e1]: Is this going to be included?

Commented [e2]: Are you going to include all of the RegRipper Reports?

- 18B302863 - Preservation Request [REDACTED]
  - 18B302863 - Preservation Request Microsoft Account [REDACTED]
  - Automatic reply 18B302863 Preservation Request Microsoft Account [REDACTED]
  - 18B302863 - Preservation Request - Consolidated Comm - [REDACTED] Bennington.pdf (Scanned copy of fax sent to CC)
- 
- Subpoena Materials
    - 18B302863 - Subpoena Request.pdf (Email dated 9.14.18)
  - Registry Explorer Updated Hives
    - 18BN05584 - EJPProductions\REG EXPLORER UPDATED HIVES\Item 2\SOFTWARE
    - 18BN05584 - EJPProductions\REG EXPLORER UPDATED HIVES\Item 2\SYSTEM

**Evidence:**

Evidence Number	Device Name	Size	Description	Status
				Imaged & Examined
				Previewed & Not Examined
				Was not Examined
				Previewed & Not Examined
				Locked & Not Examined
				Imaged & Examined
				Locked & Not Examined
				Imaged & Examined // No Evidence - Image Deleted
				Imaged & Examined
				Imaged & Examined // No Evidence - Image Deleted

**Initial Complaint:**

**Scope of Request (truncated and paraphrased):****Authority to Search:****Receipt of Evidence and Imaging:****Software Used:**

<b>Software</b>	<b>Version</b>
X-Ways Forensic - X-Ways Forensics (XWF)	19.6 SR-6 x64
Sumuri - Paladin Pro	7.01
Quantum Analytics Research - RegRipper	2.8
Eric Zimmerman - Registry Explorer	1.0.0.4
Sumuri - Carbon	3.5.1
Guidance Software / OpenText - EnCase Forensic	8.07
Microsoft - Windows 10 ( <i>main forensic computer</i> )	1803 / OS Build 17134.165 Professional
Apple - macOS Sierra ( <i>forensic laptop</i> )	10.12.6
VMWare Fusion - Professional	8.5.10 (7527438)
<ul style="list-style-type: none"> <li>• Microsoft - Windows 10 (<i>VM Testing Environment</i>)</li> </ul>	1803 / OS Build 17134.285 Professional
<ul style="list-style-type: none"> <li>• Google Chrome (<i>VM Testing Environment</i>)</li> </ul>	69.0.3497.92 64-bit
<ul style="list-style-type: none"> <li>• Avast Business Security (<i>VM Testing Environment</i>) <ul style="list-style-type: none"> <li>◦ Avast Virus Definitions</li> </ul> </li> </ul>	1809214
<ul style="list-style-type: none"> <li>• Majware Bytes Home (<i>VM Testing Environment</i>) <ul style="list-style-type: none"> <li>◦ Update Package Version</li> </ul> </li> </ul>	3.6.1.2711 (Component Package (1.0.463))
<ul style="list-style-type: none"> <li>• Webroot SecureAnywhere</li> </ul>	1.0.6931
	9.0.23.32

Microsoft - Word	Professional Plus 2013 (15.0.4420.1017)
AccessData - FTK Imager	3.4.0.5

### Summary of Findings:

### Analysis and Exhibits:

According to information provided by Det. Sharshon at the Bennington Police Department, **Item 2** was the laptop that contained the threatening user account display name. Based upon this information, **Item 2** was examined and reported on first.

#### **Item 2**

##### *External Hardware Examination*

**Item 2** was an HP 15-f387wm laptop computer. Affixed to the rear of this computer was a sticker listing a serial number of 5CD6368ZM2. An examination of the design of this laptop was completed. Due to the fragile construction of this computer, I determined that it would reduce the risk of damaging the computer by imaging the drive in-place. The tool Paladin Pro was utilized to complete this imaging task.

##### *Software & User Data Examination*

<b>Item 2 - Drive Image Details</b>	
<b>According to Paladin Pro (ewfacquire 20160424)</b>	
Manufacturer:	Seagate
Model:	ST500LT012-1DG142
Capacity:	128 GB
Serial Number:	S0NRNEAB708517
<b>According to XWF</b>	
Serial Number Match?	Could not be confirmed using XWF
Storage Capacity Match?	Yes
Disk Configuration Overlay (DCO)	No

##### *Registry Analysis - DisplayName*

The SAM, SOFTWARE, SECURITY, SYSTEM registry files were exported from Partition 3 of **Item 2**. These files were processed using the tool RegRipper.

<b>Operating System Installed</b>
Windows 10 - Home
<b>Time Zone Information</b>
Eastern Daylight Time
<b>Registered Owner</b>
[REDACTED]



<i>User Accounts</i>	
<i>Account Name</i>	<i>Last Login Date</i>
Administrator (Disabled)	9.21.2017
Guest (Disabled)	None Listed
DefaultAccount (Disabled)	None
WDAGUtilityAccount (Disabled)	None
	8.1.2018

A review of the Security Accounts Manager (SAM) registry file RegRipper tool output revealed that the user account "██████" listed a full name of "dead dead". This is the same full name that was seen in the screenshot provided by in the Bennington Police Department report. Based upon this information, the NTUSER.dat registry file was exported from the "██████" user account and processed using RegRipper.

According to the NTUSER output the timestamps on file and application activity showed that this computer was used regularly up to the July 27, 2018 date when the Bennington Police Department was contacted about this threatening display name change. An extensive timeline analysis was conducted later within this examination.

The SAM file was reviewed within XWF. According to RegRipper and XWF, this user account retained membership to the Administrators group within this system. When a user account retains Administrator level access they are permitted full access within that system.

According to XWF, the "██████" user account maintained a last write time of 7.12.2018 0624 hours (EDT). I observed that this suspicious timestamp meant that this user account was updated 15 days prior to the initial report of the threat.

07/12/2018 06:24:29.9 -4 32.8 KB SAM (ROOT)\SAM\Domains\Account\Users\000003EA \Windows\System32\config\SAM  
Screenshot 1 - SAM Last Written Date (Using XWF)

This same SAM registry file was examined using Registry Explorer. Within this tool the same timestamp of 7.12.2018 was located. The timestamp reported within this tool was UTC.

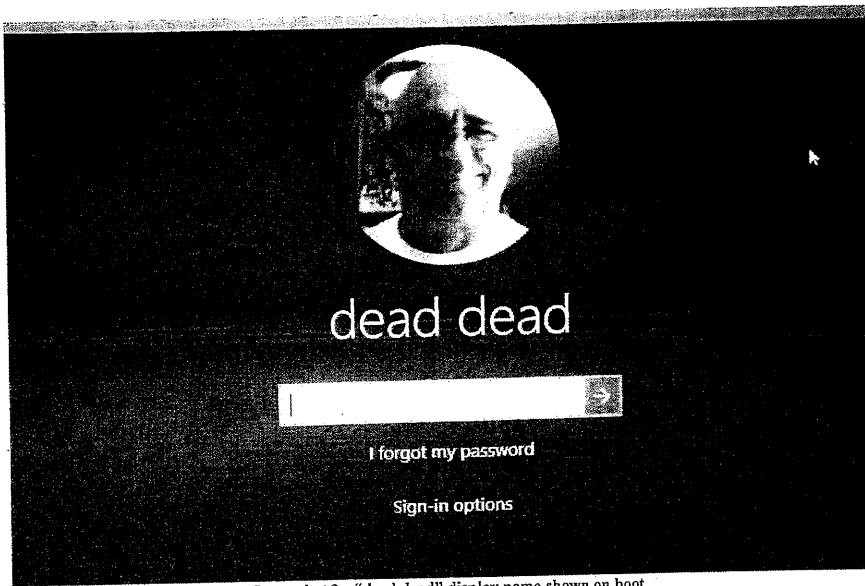
Key: SAM\Domains\Account\Users\000003EA  
Selected hive: SAM Last write: 2018-07-12 10:24:29 12 of 12 values shown (100.00%) Load complete  
Screenshot 2 - SAM Last Written Date (Using Registry Explorer)

According to the book Windows Registry Forensics 2<sup>nd</sup> edition, the author Harlen Carvey noted that the LastWrite time is updated whenever a key was created, or a subkey or value was added or deleted. According to this book, the keys within a Registry Hive can be considered similar to a folder with only the last modification time stamp reflected in the LastWrite timestamp based upon the activity of the sub-keys and values contained within it. According to an analysis of the SAM registry hive for Item 2 the user account information for the "██████" user account was stored at SAM\Domains\Account\Users\000003EA and it maintained a Last write time of 7.12.2018.

Within the SAM registry file, no timestamp information was located with a date after 7.12.2018 for this user account.

A copy of the forensic image was placed on to a sanitized portable hard drive and connected to a forensic laptop. The tool Carbon was used in order to virtually boot a copy of the **Item 2** hard drive. When a forensic image is booted, no changes are made to the actual forensic image, any interactions that an examiner has with the virtual instance of this computer are temporarily written to a cache file. When the forensic image is booted, an examiner can view the desktop and all of the files and data stored on the hard drive just as if the regular laptop itself was booted normally.

I utilized the default Carbon settings. I selected the single [REDACTED] user account that was accessible as a local user account option. I checked the domain account user list and there were no results. I was prompted with the photo image I recognized from the screenshot provided by Bennington PD as a male with glasses and a password prompt. I observed that the "dead dead" display name was still in place.

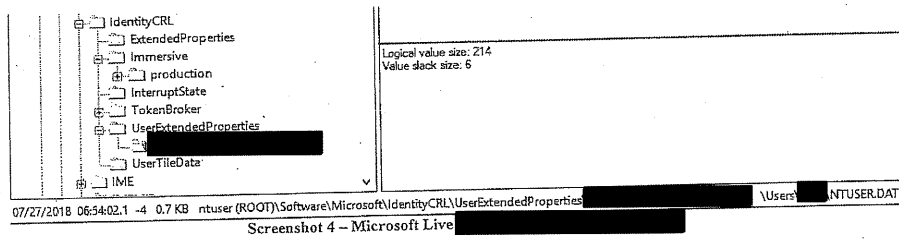


Screenshot 3 - "dead dead" display name shown on boot

I attempted to utilize the password JRL411248 that was provided by Bennington PD as the password for this computer with negative results. When I typed in the password I was presented with the following message "Your device is offline. Please sign in with the last password used on this device". When I viewed this message, I believed that this login account was associated with a Microsoft Live Account. A Microsoft Live account can be created by an individual and used to

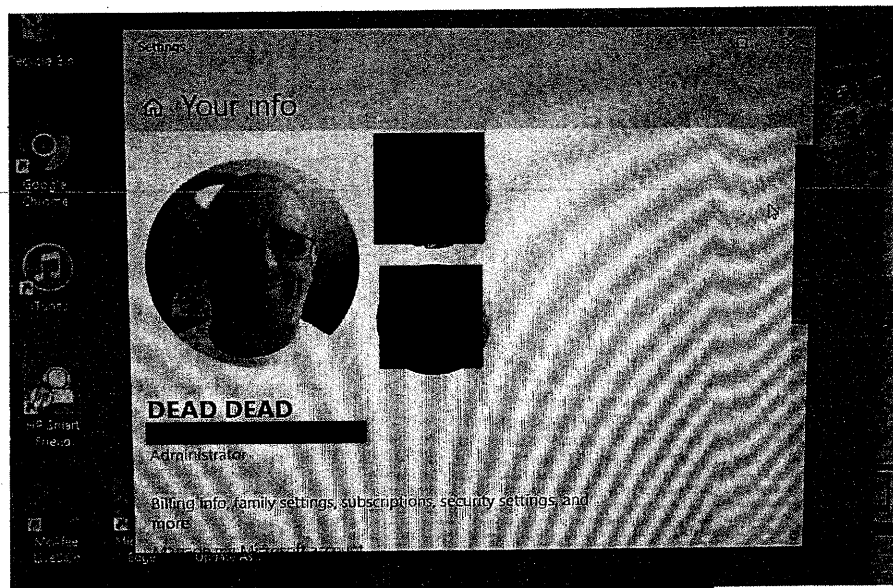
login to certain Microsoft products such as a computer running the Windows 10 operating system.

Using XWF, I reviewed the NTUSER.dat account associated with the [REDACTED] user account. According to research conducted on Microsoft TechNet, evidence of a Microsoft Live user account can be seen at Software\Microsoft\IdentityCRL\UserExtendedProperties. The email address shown was [REDACTED]



I shutdown the virtual boot of the forensic image taken of Item 2 and restarted the process. Before I initiated the boot, I utilized a setting within Carbon in order to artificially remove the password requirement from the [REDACTED] user account. I booted the forensic image of Item 2 and then I was able to login to the user account.

Once logged in, I accessed the account settings and I saw that this email address was associated with this user account. I also observed two additional pictures of unknown individuals.



Screenshot 5 – Account settings showing

Based upon this analysis, an examination of the Windows Event Logs was performed. I first used EnCase in order to review the logs. Using EnCase Item 2 was processed using several different options. A list of the processing options selected was saved to a report titled 18BN05584 - EnCase - Initial Processing Options.rtf. Once the processing was completed, the Case Analyzer function was utilized.

Using Case Analyzer I reviewed the records sorted within Accounts and Users > Account Change Event. I sorted all of the records by timestamp and Event ID. Using the publicly accessible website [www.ultimatewindowssecurity.com](http://www.ultimatewindowssecurity.com), I reviewed the Event ID list on the site for relevant IDs associated with user account changes. Within the Security Log Event ID 4738 is associated with the following action "The name of an account was changed".

At 7.27.2018 at 0826 EDT was an event log entry 4738 that showed that the following statement:

```

Dummy=-
TargetUserName=[REDACTED]
TargetDomainName=LAPTOP-D69NEDQ0
TargetSid=S-1-5-21-3192908095-2964780770-2684762360-1002
SubjectUserSid=S-1-5-18
SubjectUserName=LAPTOP-D69NEDQ0$
SubjectDomainName=WORKGROUP
SubjectLogonId=0x3e7
PrivilegeList=-
SamAccountName=-
DisplayName=dead dead
UserPrincipalName=-
HomeDirectory=-
HomePath=-
ScriptPath=-
ProfilePath=-
UserWorkstations=-
PasswordLastSet=-
AccountExpires=-
PrimaryGroupId=-
AllowedToDelegateTo=-
OldUacValue=-
NewUacValue=-
UserAccountControl=-
UserParameters=-
SidHistory=-
LogonHours=-

```

Screenshot 6 – Item 2 4781 Security Log Entry “dead dead?”

When I reviewed this log entry, I observed that there were numerous 4738 log entries. Based upon this observation, I continued to review the Security Log file using Windows Event Viewer on a forensic computer running Windows 10 Professional Version 1803. Using Event Viewer, I filtered for 4738 log entries. I observed that a total of 354 4738 log entries were located.

The date range of these log entries was from 6.27.2018 1337 hours – 7.27.2018 0826 hours. I reviewed each of these log entries and I observed that the display name for this user account was changed several times within this timespan. I created a table that identified the display name and the date range that this name was reportedly in-place.

Earliest Date Located	Latest Date Located	DisplayName
7.12.2018 0624 hours	7.27.2018 0826 hours	dead dead
6.28.2018 0737 hours	7.11.2018 2149 hours	James Lawton
6.27.2018 0820 hours	6.27.2018 0820 hours	<i>No Display Name Listed</i>
6.27.2018 1337 hours	6.27.2018 2019 hours	chicken nugget

From this breakdown I was able to identify that the display name “dead dead” was actually in place and appeared to remain in place since 7.12.2018. This was an additional 15 days earlier than the 7.27.2018 initial report of this incident made to the Bennington Police Department. According to this analysis a total of 4 different display names were in place when you include the 6.27.2018 to 6.28.2018 timespan when there was no display name listed.

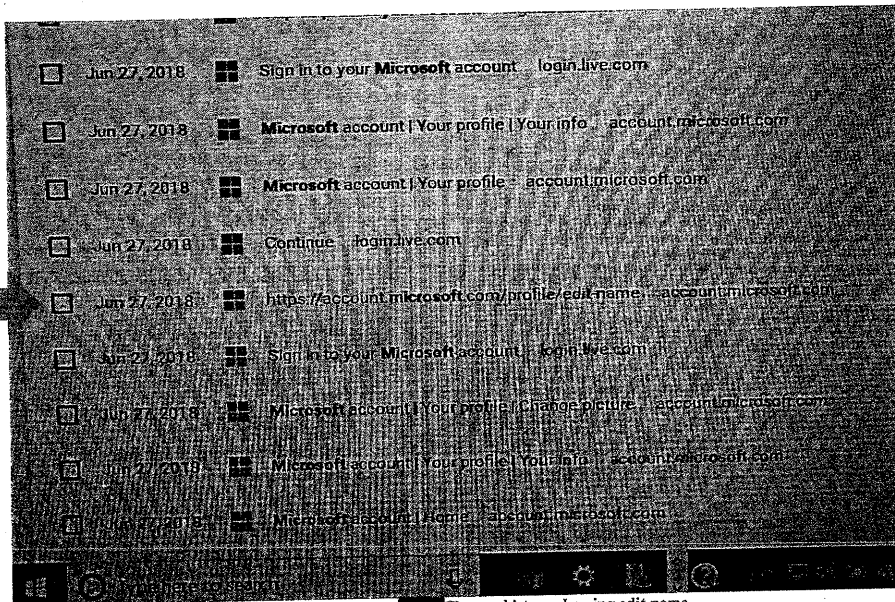
Based upon this analysis, I utilized IEF to process both **Item 1A** and **Item 2**. A list of the processing options selected were placed into a text file called 18BN05584 - IEF Case Information and Processing Options.txt. Once processed, I conducted a global filter for the timestamps 6.26.2018 0000 hours – 7.28.2018 2359 hours against all artifacts that were identified by the IEF processing of both items. At the completion of this filter, a restriction was placed to only show information from **Item 2**.

I reviewed the web history stored on **Item 2** and I observed several web history entries associated with the Google Chrome web browser that showed that on 6.27.2018, this computer accessed the website <https://accounts.microsoft.com> and websites such as [account.microsoft.com/profile](https://account.microsoft.com/profile).

One entry on 6.27.2018 at 1855 hours (EDT) showed the web entry <https://account.microsoft.com/profile/edit-name>

This information was bookmarked and exported into 5 different .CSV spreadsheet reports within a directory titled CSV Export 2018-09-12\_13-55-47.

Using Carbon, I opened up the Google Chrome history on the [REDACTED] user profile and I observed the same edit-name web traffic that was seen using IEF.



Screenshot 7 – Item 2 – [REDACTED] Chrome history showing edit name

*Microsoft Live Account Preservation*

On September 6, 2018, I contacted the Microsoft Corporation and spoke with representatives at the Digital Crimes Unit (DCU). They advised me that they retain various types of data associated with a Microsoft Live account. They stated that they do not track or retain changes to the display name for a user account. They did state that they do track login activity with timestamps and associated Internet Protocol (IP) addresses. Based upon this information, I contacted Det. Lt. Lancé Burnham who authorized that I send this preservation letter to Microsoft at the email address uslerq@microsoft.com. This letter was sent on September 6, 2018. A copy of this preservation letter was filed with this case as 18B302863 - Preservation Request

██████████ The case number 18B302863 reflected the Vermont State Police case number assigned to this case.

On September 7, 2018, I contacted Microsoft DCU and spoke with representatives who confirmed that they received this request and that they will process it in the order that it was received.

On September 13, 2018, I did not receive any preservation request confirmation message or any internal case identification numbers. I contacted Microsoft DCU and spoke left a message requesting a call back.

On September 14, 2018, I was contacted by Microsoft DCU who advised me that they have an internal case number of GCC1074742S6Q9V3.

*VM Testing*

Based upon these observations a testing environment was setup. A Windows 10 Professional virtual machine (VM) was built and accessed using VMWare Fusion Pro. A version of the Windows 10 Home edition was not available at the lab in order to conduct a test using the exact edition. I know that both Windows 10 Home and Windows 10 Professional both record events so all testing was completed using the Professional edition.

The tests that were completed in order to examine the changes that take place within a known environment. Within the testing environment, the following four interactions were completed.

1. Converting a local user account to a Microsoft Live user account
2. Change the name of the Microsoft Live user account via the website interface. Note any observable changes were applied to the local machine
3. Restart the system and note any observable changes that were applied.
4. Attempt to change the name using any local interface without using advanced techniques.

A table with timestamps was created in order to document the steps taken to complete the series of tests. The spreadsheet used to create the table within this report was filed with this case as 18BN05584 - Test VM Timeline notes.xlsx.

#### 9.13.2018 Test

Time	Interaction
1038	Clicked sign-in with account
1043	Logged in provided test password for local user account "abc123"
1043	Created PIN "123789"
1043	Test Microsoft Account "Monty Car" vermont47@outlook.com was configured to the test VM
<b>VM Snapshot Taken</b>	
1102	Used test VM event viewer to review changes
	Located at 4738 log entry timestamped 1043 DisplayName = "Monty Car"
1115	Added share folder to local Apple forensic laptop and exported logs
<b>VM Snapshot Taken</b>	
1124	Accessed Microsoft Account via Chrome
	Observed same "edit-name" URL seen in Item 2 Chrome traffic
1124	Changed name on website to "Monty Green"
1129	Observed that this changed was not immediately applied to the VM
1137	No change / Restarted VM
1146	Upon Restart, change was immediately seen before a login was even completed
<b>VM Snapshot Taken</b>	
1159	VM Test Shutdown
1226	System Started. Check for local ability to change name was completed

At the completion of this series of tests, the following information was learned. The conversion of a local user account to a Microsoft Online account is a seamless process that presents to the user that it is performed completely within the Windows 10 environment.

The initial conversion of the account from a local user account to a Microsoft Live user account brought the initial changes to the system including the updating of the "test" user account to show a display name of "Monty Car".

Based upon testing, it appeared that without the use of uncommon advanced techniques such as using the command line or manually editing the Windows Registry it did not appear possible to change the name without accessing the accounts.microsoft.com website.

Once a Microsoft Live account was configured, changing the name using the website did not create any immediate changes that were visible to the user. The name remained the same old name "Monty Car". A period of time was waited and the "Monty Green" change was not visible.

A restart of the test virtual machine was completed and the name change was immediately visible at the login screen without even logging into the system.



An analysis of the Security event logs for this test system showed the same 4738 Event IDs that reflected the updated DisplayName data.

At the completion of this test, I spoke with Agency of Digital Services Technician Drew Emory. Mr. Emory informed me that he had a Microsoft Live account. I asked Mr. Emory to change his displayed name for his profile without using any advanced techniques. I provided no context to this request because I wanted Mr. Emory to work to perform this change using any standard method he was aware of. I observed as Mr. Emory navigated to the Control Panel and settings of his system and I observed that he was unable to find a way to change this name without being connected to the Internet and interacting with the Microsoft Live website.

#### *Registry Analysis – Network History*

On September 13, 2018, Det. Lt. Burnham informed me that members of the Vermont State Police spoke with Ms. Ruqaiyah Morris [REDACTED]. According to Ms. Morris, Item 2 used and operated by Mr. Lawton rarely left their home at [REDACTED] Bennington, Vermont.

A physical examination of Item 2 during the time that it was at the lab showed that this computer maintained an Ethernet network port and a wireless network card capability. This was documented in lab photos IMG\_8176.JPG and IMG\_8177.JPG. An examination of the Windows Registry specifically for the purposes of learning the connectivity history of this device was performed in order to assist in establishing a connection history timeline.

The SOFTWARE registry hive as well as the associated SOFTWARE.log files were exported from the forensic image of Item 2 and loaded into Registry Explorer. Registry Explorer utilizes the associated .LOG files that are associated with the respective hives in order to present the data to an examiner.

When the Windows Operating System acts to make a change to a Registry file, it first writes this change to a log file. This action is done in order to maintain system stability. Within the log file the intended change as well as the method the system can use to reverse the change is logged. When the system can commit the change, the change is updated to the live Windows Registry file held in running memory. During a forensic analysis of an offline system, these files are represented for example as SOFTWARE, SOFTWARE.LOG1, SOFTWARE.LOG2.

Using Registry Explorer, the tool creates an updated hive that contains the cumulative changes from the associated log files and combines all of this information into a single new hive file. This new hive file was titled SOFTWARE and it was saved with this case at the following location 18BN05584 - EJPProductions\REG EXPLORER UPDATED HIVES\Item 2\SOFTWARE.

The first area examined was the network list located at SOFTWARE: Microsoft\Windows NT\CurrentVersion\NetworkList. The following information was located:

Network Name	First Connect LOCAL	Last Connected LOCAL	Gateway Mac Address
BLASC Production	2017-09-21 14:11:42	2017-09-21 14:11:42	00-18-0A-86-C3-00
xfinitywifi	2017-11-22 04:05:58	2018-05-30 07:34:10	F4-3E-9D-03-68-55
NETGEAR	2017-10-27 12:23:51	2018-06-24 14:08:37	A0-21-B7-B1-D4-99
fairpoint09208	2018-06-24 17:26:43	2018-07-27 10:05:22	D8-B6-B7-BA-EC-58
NETGEAR 2	2017-12-09 11:10:14	2018-06-17 22:00:26	D8-B6-B7-82-47-55
DIRECT-AI LAPTOP-D69N	2017-12-24 15:51:57	2017-12-25 06:33:08	

This information showed that there were several networks that this laptop connected to within 2017 – 2018. This wireless information appeared to be consistent with the information provided by Ms. Morris that this laptop did not often leave the residence often. This information reportedly showed that on June 24, 2018 the wireless network NETGEAR was connected. This was 3 days before evidence of the DisplayName “Chicken Nugget” was observed in the Event Logs.

On July 27, 2018 at 1005 hours, the wireless network fairpoint09208 was connected to. The last user account entry of “dead dead” was shown within the Event Logs at 0826 hours.

The Gateway MAC Addresses for this list were researched using the publicly accessible website Arul’s Utilities <http://aruljohn.com/mac>. According to this lookup site, the 5 Gateway MAC addresses resolved to the following chip manufacturers:

Network Name	First Connect LOCAL	Last Connected LOCAL	Gateway Mac Address	MAC Vendor
BLASC Production	2017-09-21 14:11:42	2017-09-21 14:11:42	00-18-0A-86-C3-00	Cisco Meraki
xfinitywifi	2017-11-22 04:05:58	2018-05-30 07:34:10	F4-3E-9D-03-68-55	Benu Networks, Inc.
NETGEAR	2017-10-27 12:23:51	2018-06-24 14:08:37	A0-21-B7-B1-D4-99	NETGEAR
fairpoint09208	2018-06-24 17:26:43	2018-07-27 10:05:22	D8-B6-B7-BA-EC-58	Comtrend Corporation
NETGEAR 2	2017-12-09 11:10:14	2018-06-17 22:00:26	D8-B6-B7-82-47-55	Comtrend Corporation
DIRECT-AI LAPTOP-D69N	2017-12-24 15:51:57	2017-12-25 06:33:08		

I know through training and experience that MAC Vendor information relates to the information known by registration entities about the actual network card installed or configured within a device. It is possible with a degree of technical savviness to edit or modify a MAC address and that it is possible that this information may not be up-to-date or accurate.

*Subpoena Request* - [REDACTED]

On September 14, 2018, I authored a subpoena request to the Bennington County States Attorney Office requesting subscriber and login history for the user account [REDACTED]

This request was made based upon the analysis of **Item 2** as well as statements made by Mr. Lawton that an unknown individual completed the change to his Microsoft Live Account.

On September 17, 2018, I was advised by Bennington County States Attorney Erica Marthage that her office would process this subpoena request and report back when it has been completed.

On September 18, 2018, I received a copy of the authorized subpoena from the Bennington County States Attorney Office.

On September 20, 2018, I sent a copy of the signed subpoena received from the Bennington County States Attorney Office to Microsoft Corporation for processing. This subpoena was sent to the [uslreq@microsoft.com](mailto:uslreq@microsoft.com) email address per the instructions found within the publicly accessible website [Search.org](http://Search.org). Within the body of the email and within the subpoena itself was the Microsoft Internal Case Number GCC1074742S6Q9V3. I immediately received an automated email reply from Microsoft that stated that they received the email.

*Preservation Request – ISP Consolidated Communication* - [REDACTED]

On September 13, 2018, I was advised that the Internet Service Provider (ISP) servicing the residence [REDACTED] Bennington, Vermont was Consolidated Communications. I know from experience that this Internet Service Provider provides services to numerous areas throughout the State of Vermont.

On September 14, 2018, based upon this information and the information learned during this analysis, I authored a preservation request to Consolidated Communications. I contacted the Consolidated Communications Security Department and spoke with representatives. They provided me with a contact number for Alicia Rakstad at 916.746.3007. I contacted that number and left a voicemail message. The message stated to fax legal process to 916.773.5776. I utilized the publicly accessible website [Search.org](http://Search.org) and learned that this was the same fax number listed for Consolidated Communications. I faxed this preservation request to the number listed.

On September 19, 2018, I was contacted by Det. Lt. Lance Burnham regarding this matter. Det. Lt. Burnham asked how an individual could identify their Internet Protocol (IP) Address for a given connection. Det. Lt. Burnham provided me with the IP Address 192.168.1.7 and he advised me that the victim Ms. Morris provided investigators with this and stated that it was her IP Address. I informed Det. Lt. Burnham that this was an internal IP Address and that for this specific investigation knowing the external IP Address would be important. I provided Det. Lt. Burnham with the publicly accessible Internet website [ipchicken.com](http://ipchicken.com). I explained that this website would quickly provide an individual with their external IP Address. A few moments later, Det. Lt. Burnham provided me with a screenshot image file titled [IMG\\_2147.jpeg](#). I

recognized that the IP Address 64.222.152.250 was an external address that would be routable on the Internet. This screenshot was printed and filed with the case.

On September 21, 2018, I attempted to contact Ms. Alicia Rakstad at Consolidated Communications. I left a voicemail message with the 916.895.9674 number I was provided earlier by the Consolidated Communication Security Department. I also called the 916.746.3007 number listed for Ms. Rakstad with no results. I will continue to follow-up on this.

XXXX CONFIRM RECEIPT AND INTERNAL CASE NUMBER IF AVAILABLE. XXXX

*Additional Registry Analysis – NTUSER.DAT & USRCLASS [REDACTED]*

A review of the NTUSER.dat file for the user profile [REDACTED] was completed. This file was processed earlier using RegRipper. This output was reviewed using Microsoft Word. The RecentDocs section was examined with no suspicious activity observed.

The UsrClass.dat registry file associated with the user profile [REDACTED] was completed using Shellbags Explorer. Shellbags within the Microsoft Operating System are pieces of data utilized by the Windows Operating System in order to track a variety of user interactions including window sizes and layout preferences. Within a forensic analysis, Shellbags can reveal to an examiner where a user profile navigated within Windows. I observed no suspicious activity present.

*Additional Registry Analysis – SECURITY*

The SECURITY registry hive was examined with no suspicious activity present.

*Additional Registry Analysis – RegBack registry files.*

I navigated to the /SYSTEM32/CONFIG/REGBACK directory and I observed that the RegBack files were empty. This was consistent with publicly accessible research stating that after the 1803 major update to Windows 10 in 2018 the RegBack files are no longer maintained. This was confirmed by examining a forensic computer using FTK Imager that had previously had the 1803 update applied. A data carving operation for all registry file types was completed using XWF. I reviewed the artifacts recovered on Partition 3 the main data partition with no suspicious activity located.

*Windows Share Settings*

I examined the Windows Share settings for **Item 2** using Registry Explorer. Exploring the updated SYSTEM hive created earlier during this analysis at ControlSet001\Services\LanmanServer\Shares showed no user created Windows Shares were visible. Using Carbon, I accessed a command prompt of the virtualized version of Item 2. Typing in NET SHARE presented me with a list of all shared areas on the system. I observed that only system default shares were in place.

*Security Settings / Antivirus & Malware**Windows Defender & Firewall*

The Windows Defender Antivirus Log was reviewed. This log was titled Microsoft-Windows-Windows Defender%4Operational.evtx. Within this log was an entry for 7.27.2018. This listed that the antivirus system client was up and running in a healthy state. The version information for this log entry listed the system as having the following details:

Platform version:	4.18.1806.18062
Engine version:	1.1.15100.1
Signature version:	1.273.422.0

According to publicly accessible research, at the time of this analysis 9.18.2018 the signatures list was 1.275.1448.0. There were a total of 849 events logged within this Windows Defender log file.

**LEFT OFF AT THE FOLLOWING ACTIONS FOR THIS SECTION. REVIEW THE WINDOWS DEFENDER LOG INFORMATION AND NOTE ANY SUSPICIOUS UP/DOWN TIME RELEVANT TO THE TIME THAT THE NAME CHANGES TOOK PLACE.**

**REFER TO LATEST NOTES FOR NEXT SECTION WORK.**

*Avast Business Security*

The forensic image for **Item 2** was transferred to a sterile external hard drive and connected to a fully patched virtual machine running Windows 10 Professional. Within this virtual machine a copy of the security tool Avast Business Security was installed within it. This is a security tool that was paid for by the Vermont Department of Public Safety for their regular use. This tool was fully updated to include the latest virus definitions and program features. The forensic image for **Item 2** was virtually mounted using FTK Imager. Once mounted, I accessed the settings for Avast Business Security. Within the settings I selected to scan all files in a full scan in-depth mode. Additional settings for testing whole files and to flag for potentially unwanted programs were selected.

A full scan of the virtually mounted forensic image of **Item 2** was completed with no issues reported.

*Malware Bytes Home*

The scanning process was repeated using the tool Malware Bytes Home. This tool was installed on the same virtual machine and fully updated. The scan within archives was selected, scan for rootkits, and identify potentially unwanted programs were additionally selected options. A scan was completed with no reported threats having been detected.

*Webroot SecureAnywhere*

The scanning process was repeated using the tool Webroot SecureAnywhere. This tool was installed on the same virtual machine and fully updated. A deep scan was selected against **Item 2**. This scan was completed with no threats detected.

NEED TO UPDATE REPORT TO REFLECT INFORMATION IN SUPPLEMENTAL REP

**Item 1 & Item 1A**

*External Hardware Examination*

**Item 1** was an Asus R554L laptop computer. Affixed to the rear of this computer was a sticker with a possible serial number of FBN0WU134456464. Also located was a detail that stated "Vermont Computer Co Kiah Morris [REDACTED]". Contained within **Item 1** was a single 2.5 inch hard drive. This hard drive was removed and processed separately as **Item 1A**.

**Item 1A**

Item 1A - Hard Drive Details	
<b>According to Drive Label</b>	
Manufacturer:	Samsung
Model:	MZ-7PA1280/0D1
Capacity:	128 GB
Serial Number:	S0NRNEAB708517
<b>According to XWF</b>	
Serial Number Match?	Yes
Storage Capacity Match?	Yes
Disk Configuration Overlay (DCO)	No

*Software & User Data Examination*

<i>Operating System Installed</i>	
<i>Time Zone Information</i>	
<i>Operating System Install Date</i>	
<i>Last Shutdown</i>	
<i>Registered Owner</i>	
<i>User Accounts</i>	
<i>Account Name</i>	<i>Last Login Date</i>

Closing Comments

Supporting documents, image file paths, and various other file types have been bookmarked and are available in additional analysis software-generated reports.

---

All documents and references in this report have been provided to the case agent. This report is a synopsis of the findings, to date, conducted on the digital media referenced in this report based upon the searches identified. This report may not be inclusive of all potential evidence contained on the digital media referenced in this report. Any additional analysis conducted on the referenced digital media will be documented in future reports.

End of report.

Analysis Start: XX/XX/XXXX

Analysis Completion: XX/XX/XXXX

08/01/18  
15:34

Bennington Police Department  
LAW Incident Table:

Page: 587  
1

Incident  
Incident Number 18BN05584 Nature Threatening  
Case Number Image  
Address [REDACTED]  
City Bennington State VT ZIP 05201  
Area 0202 BENNINGTON Contact James

Complainant  
Numbr 101122  
Last Lawton Fst James Mid R  
DOB [REDACTED] SSN - - Adr [REDACTED]  
Race W Sx M Tel [REDACTED] Cty Bennington ST VT ZIP 05201

Details  
Offense/Statute PSC Reported 0470 Observed PSC  
Circumstances LT20  
Rspndg Officers Sharshon, Micha  
Rspnsbl Officer Sharshon, Micha Agency 0202 CAD Call ID 6473425  
Received By Howe, Brian Last RadLog 14:15:37 07/27/18 CMPLT  
How Received T Telephone Clearance RFA Ready for Approval  
When Reported 14:04:38 07/27/18 Disposition ACT Disp Date 07/27/18  
Occurrd between 14:04:27 07/27/18 Judicial Sts  
and 14:04:27 07/27/18 Supervisor  
MO

Narrative  
Narrative (See below)  
Supplement

=====

INVOLVEMENTS:				Relationship
Type	Record #	Date	Description	
NM	1623776	07/30/18	Morris, Ruqaiyah K	Spouse/Partner
NM	1841252	07/30/18	Misch, Max B	POI
NM	101122	07/27/18	Lawton, James R	*Complainant
CA	6473425	07/27/18	14:04 07/27/18 Threatening	*Initiating Call

LAW Incident Offenses Detail:

Seq Code	Offense and Statute Codes	Amount
	Statute Code	
1	PSC Suspicious Person/Circumstance	0.00



LAW Incident Circumstances:  
Contributing Circumstances  
Seq Code Comments  
1 LT20 Residence/Home

LAW Incident Responders Detail  
Responding Officers  
Seq Name Unit  
1 Sharshon, Micha M367

--- Main Radio Log Table: ---

Time/Date	Typ	Unit	Code	Zone	Agnc	Description
14:15:37 07/27/18	1	M367	CMPLT	0202	0202	incid#=18BN05584 Completed cal
14:07:08 07/27/18	1	M367	ARRVD	0202	0202	incid#=18BN05584 Arrived on sc

Narrative:

BENNINGTON POLICE DEPARTMENT NARRATIVE

18BN05584

Nature of call: Suspicious

Date & Time Reported: July 27, 2018, 1404 Hours

Location of Call: [REDACTED], Bennington, Vermont

Narrative:

On Friday, July 27, 2018, at approximately 1404 hours, I took a phone call regarding suspicious circumstances.

I spoke with James Lawton, [REDACTED], who advised me that he and his wife Ruqaiyah Morris, [REDACTED], were having issues with a person he described as a "local neo-nazi". Lawton advised me that this male, later identified to me as Max Misch, [REDACTED], was causing issues for them online as well as for his computer. I asked Lawton to expound upon the issues for me.

For the first issue, Lawton advised that Misch harasses Morris online, via social media. He said that Misch targets Morris specifically, making unpleasant comments on various social media platforms. For reference in this report, on Facebook Misch goes by "Max Misch" and Morris goes by "Kiah Morris VT State Representative", and on Twitter Misch's handle is "maxmisch83" and Morris's handle is "kmrhapsody". I was provided with screenshots from Twitter and Facebook. The Twitter posts has no timestamp and the Facebook had a timestamp of January 26 (no year). I reviewed the posts from Misch, which are very are strongly political. However, there did not appear to be any specific call-to-action, threats, or call for violence against Morris. The only action Misch claimed he would do was "troll" Morris at a rally. Trolling is a term for actions meant specifically to annoy an individual or a group of people. Trolling is usually mean-spirited, however it is generally not criminal in nature. It should be noted that the screen shots from Twitter do not show the entirety of the conversation, mostly responses from Misch. This is because either Lawton or Morris did not provide the totality of the conversation. The images have been attached to this report and filed in the to-be-filed hopper in the Bennington Police Dispatch Center.

I inquired about the issue with Lawton's computer. Lawton advised me that when he turned on his computer in the morning and got to the log in screen, where his account name normally is was replaced with "dead dead" instead of "James Lawton". He advised me that he notified Morris of this, who was in a legislative session at the time. Lawton said that Morris had been speaking with the Vermont State Police and that it was his understanding that the State Police would take the computers. Lawton asked if he should bring the computer to the Bennington Police Department, which I advised him no. I advised Lawton to contact Morris and see what the Vermont State Police wanted her to do with the computer. Lawton acknowledged this and thanked me for my time.

On Monday, July 30, 2018, it came to my attention that Lawton's computer was delivered to the Bennington Police Department. I spoke with Det. Cole and filled him in with as much of the situation as I was aware of. Det. Cole suggested I contact the Vermont Internet Crimes Against Children (ICAC), who regular do forensic analysis on computers.

I spoke with Eric Jollymore at ICAC, who advised me that a situation that Lawton

encounter is possible, however it would require whoever did it to have an advanced degree of technical knowledge of computers.

It was determined that the computers would not be forensically analyzed.

At this time, I am sending this report down to the Bennington County State's Attorney's Office, as well as a copy of the Misch's internet posts, for review for disorderly conduct via electronic device. (T.13 VSA 1027).

Case Status: Active

Submitted: M. Sharshon 8/1/2018

---

Keith Morris VT State Representative

- Page
- Inbox
- Notifications
- Insights
- Publishing Tools
- Promotions

Settings

Help

Miss Misch

Jan 26



Miss Misch

Jan 26

MAX MISCH POSTS ABOUT COMMENTS



Max Misch  
You blocked me on Twitter instead of

Jan 26



Max Misch · Keith Morris VT State Representative  
January 26 · 0

You blocked me on Twitter instead of debating me, one of your constituents and an Iraq veteran. I didn't attack you personally with hateful epithets or anything like that. Typical of the left.

Stop trying to make Berrington look like the crime-ridden streets of Chicago, where you're from, or Mogadishu. By bringing the ICE raid to 601, violent Somali "refugees" who also test positive for active tuberculosis. We don't want that kind of "cultural enrichment" contrary to what you might think.

Google Mohamed Noor. He was a Somali police officer in Minneapolis who shot and killed an unarmed woman through his police car in 2017. She was just trying to report what she believed was a sexual assault in the vicinity.

Google Abdul Arfan. He was a Somali "refugee" who used his car and a knife to sexually assault 13 people on the CSU campus in 2016.

Google Somali hate gangs. Too many examples to list here.

Type here to search





### Comments

criminal justice system is broken. In my speech, I talked about the fact that I don't vote for my personal interests, I vote for what is best for all Vermonters. And that those laws I vote for may well protect even you from having to experience greater criminality. That those laws I work to put in place may help those who have caused harm rectify their wrongs through restorative justice instead of the prison system. Because that is what we are elected to do and those are the values I represent. You are welcome espouse white nationalist, neo-nazi views and opinions in public forums - that right is guaranteed by the constitution. And I have the right to take whatever steps are necessary to protect me and my family from the impacts of your use of hate speech.

3d Reply



**maxmisch83 @kmrhapsody** Bullshit. Instead of just having thicker skin and shrugging off the tweet, you tried to have me arrested and put in prison for having the audacity to mock you online. What "impacts" of my "hate speech" would you need protection from? You're full of shit and I will do my best to inform everyone of your agenda to imprison anyone who makes fun of you or disagrees with you, like the left in general. I already know at least one well-respected member of the community who is making plans to stop you winning by default because you run unopposed each time.





4h Reply





Add a comment...





### Comments

 **kmrhapsody** @maxmisch83 you first. 



5d Reply

 **maxmisch83** @kmrhapsody It's incredible that you'll complain about VT being too white after moving here precisely because it's one of the whitest in the country and therefore has one of the lowest crime rates per capita in the country, basically the opposite of the multicultural hellscape of Chicago, where you're from, which has one of the highest amounts of homicides in the nation. 


5d Reply

 **kmrhapsody** @maxmisch83 Why are you obsessed with me? 

5d Reply

 **maxmisch83** @kmrhapsody I'm obsessed with keeping my town, state, and country safe while you're obsessed with doing the opposite. I'm trying to defend Western civilization while you're trying to destroy it. You're the epitome of why the GOP will be victorious in the midterms this Nov and then in 2020. You and your leftist comrades like Schumer, Blumenthal, Pelosi, etc. should continue doing what you're doing! 🇺🇸 

5d Reply


 **kmrhapsody** @maxmisch83 See again



Add a comment...




## Comments

 maxmisch83 @kmrhapsody Lol @ believing blacks are still oppressed in 2018. How about you start to "dismantle racism" by telling your racial brethren to stop attacking random old white people, unprovoked, such as this 8 on 1 brutal assault which occurred recently.




<https://abc7news.com/berkeley-police-need-your-help-finding-suspects-accused-of-beating-72-year-old-man/3783641/>


2h Reply

 maxmisch83 @kmrhapsody Spare me the semantic sophistry. You can't deny that you called the police, FBI, and state attorney because I hurt your fragile feewings after your hard-fought electoral victory against no opponent, using the vernacular of your kinsmen. Bottom line, you have no real arguments against my "hate" based on actual facts, stats, and data, so you instead choose to try to silence people like me who are dissident voices. Well, you failed. You will never silence me. Every time you attend a political rally at the Four Corners or another local venue and I'm aware of the event, I will troll the hell out of you and the other subversives there. Maybe I'll bring a friend or three with me too.



1h Reply

 maxmisch83 If you feel different and like you

 Add a comment...



Following

You



maxmisch83 liked your post. 10h



maxmisch83 commented: The only reason she's an elected "representative" over here is because she's been running unopposed. 10h



maxmisch83 commented: I agree. Families belong together in detention facilities because they're committing crimes. Nobody wants to separate families. We want them all to go back to their shitholes together. 10h



maxmisch83 commented: Stop using children for your subversive political agenda, making them hold signs when they don't truly understand the issues. You want families to stay together? Tell them to stay in their own country and stop with their fake "asylum" and "refugee" nonsense. Instead of trying to illegally come here, they should improve their own countries if they're shitholes. 11h



maxmisch83 commented: Stop pushing "social justice" on your nearly entirely White constituency in Bennington, VT. Go back to Chicago if you want to engage in SJW bullshit. We will continue to fight against your efforts to make our town/state look more like your ugly mongrel son. 11h



brooklynrepro liked your post. 11h







dead dead