PLANES, TRAINS, AND AUTOMOBILES: THE METADATA OF INSURRECTION

Kevin Douglas Creek, whose arrest was announced yesterday, is your garden variety January 6 defendant accused of assaulting cops in the extended fighting on the West Terrace that day.

But his arrest affidavit is a lesson in all the ways that insurrectionists, or any other travelers, leave a path of metadata that can be tracked later.

While the FBI described that someone reported comments Creek made in a visit to the Northside Forsyth Hospital days after the riot — Creek said that, "he was gassed before in the military where he never experienced the types of effects he was experiencing this time" — it appears that no one tracked down that tip directly (many of those who were gassed on January 6 would have only weak trespassing cases against them).

It seems likely that Creek was identified anew based off his Be on the Lookout pictures captured from two alleged assaults against cops. The affidavit doesn't say he was identified through facial recognition, but the inclusion of the two clearest BOLO pictures of him in the affidavit suggests that's likely.

Investigators often use driver's license pictures to match for facial recognition, and indeed, this affidavit describes validating Creek's BOLO to his Georgia driver's license (though not the use of facial recognition to get there).

> Your affiant reviewed a driver's license photo issued to Creek and the Facebook profile photos posted by Kevin Creek and also compared these to images and videos of AFO-296. By comparing these photographs to the videos and images from the U.S. Capitol, your affiant believes the images are all consistent with Kevin Douglas Creek.

Once they IDed Creek as a suspect, they started accumulating proof of his travel. While Creek drove to insurrection, Air Marshals at Atlanta's airport nevertheless witnessed Creek entering his F-150 at the airport, which tied him to his license plate.

> Your affiant reviewed records obtained from open sources and verified that a F-150 Supercrew with license plate ending in XXX5830 is registered to Creek. Federal Air Marshals have also observed Kevin Creek entering this vehicle at the Hartfield Jackson

> International Airport in Atlanta, Georgia.

Once they tied Creek to his license plate, they tracked his drive to DC.

> This license plate was run by an FBI-Atlanta Task Force Officer through Leonardo, a Automatic License Plate reader in Georgia. Leonardo automatic plate reader captured Creek driving to D.C. from Georgia on at 8:44 am on January 5, 2021 and returning at 6:11 pm on January 7, 2021. On both occasions, the reader registered the license plate on I-85 in Franklin County, Georgia.

Given Franklin County's location on the border with South Carolina, Georgia's license plate reader probably picked up Creek on his way into South Carolina on I-85 on January 5 and on his way back into Georgia on January 7.

Along the way, his credit card purchases showed him buying gas going and returning.

> For example, on January 5, 2021, Creek used his credit card at Shell Oil in Petersburg, VA, Quinns in Arlington, VA and at Panera Bread in Burlington, NC. On January 7, 2021, Creek used his credit card at QT in Anderson, SC and at BP in North Chester, VA.

His credit card not only placed him at what was then a Courtyard in Arlington, but showed that he took the metro into the city on January 6.

> Travel records obtained from Washington Metropolitan Area Transit Authority confirm that on January 6, 2021 at 8:15am, Creek's credit card was used to purchase four metro cards. These metro cards were used to traveled from Rosslyn Station McPherson Sq Station at approximately 8:17 am. At 11:07 am, one

> metro card was used to return to Rosslyn Station from McPherson Station. The other 3 cards returned from Arch-Navy Memorial Station to Rosslyn Station at 4:37 pm.

This tipped off the FBI that three people were traveling with Creek. Creek told the FBI whom he traveled with in an interview on May 21, but if he hadn't, the FBI would have been able to use surveillance video from the hotel and the Metro to figure out who the others were, especially the two that appear to have left the Capitol with him shortly before 4:37PM.

At the beginning of this investigation, there was a focus on how many rioters had IDed themselves on social media. In Creek's case, he may have deleted his live streaming from the attack before anyone chased down the tip based off his hospital visit (FBI ran some kind of GeoFence off of people live streaming to Facebook from *inside* the Capitol, but it's not clear Creek ever entered the building).

> An open source search was conducted to identify any social media accounts in the name of Kevin Creek. A search of Facebook revealed an account with the handle Kevin Creek. This Facebook profile shared a photo of a "Nailed It Roofing and Restoration" business card. Nailed It Roofing and Restoration is registered with the Georgia Corporations Division with a registered agent of Kevin Douglas Creek.
>
> [snip]
>
> Initially, Creek told affiant he was live streaming January 6th and posted the stream and photos on his Facebook account. Creek deleted those photos once he returned home. Creek stated he may have heard about the protest from his twitter account (handle @KevinDCreek) but stated he could not remember for

> certain.

As described then, the only lead the FBI got from Creek's Facebook was the tie to his business, "Nailed It Roofing and Restoration."

But even without leaving boasts on Facebook for the FBI to find, Creek nevertheless left a clear trail of metadata in his wake as he traveled to insurrection.

Update, June 18: The government is not opposing a motion to revoke Creek's detention order, citing (among other things), his "significant cooperation with law enforcement" since he was first interviewed.