ROBERT S. BREWER, Jr.
United States Attorney
ANDREW P. YOUNG
Illinois Bar No.: 6284303
BENJAMIN J. KATZ
California Bar No.: 272219
Assistant U.S. Attorneys
Office of the U.S. Attorney
880 Front Street, Room 6293
San Diego, CA 92101
Tel: (619) 546-7981
Email: Andrew.p.young2@usdoj.gov

Attorneys for the United States

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA, Plaintiff, v. VINCENT RAMOS Defendant.	Case No.: 18-CR-1404-WQH Date: May 28, 2019 Time: 9:00 a.m. **UNITED STATES' SENTENCING MEMORANDUM**

The UNITED STATES OF AMERICA, by and through its counsel, ROBERT S. BREWER, JR., United States Attorney, and Andrew P. Young, and Benjamin J. Katz, Assistant United States Attorneys, hereby files its Sentencing Memorandum.

I.
INTRODUCTION

Vincent RAMOS (hereinafter the "Defendant" or "Ramos") was the CEO of Phantom Secure, a Canadian company that provided encryption and other services to Transnational Criminal Organizations ("TCOs") for the specific purpose of evading and impeding law enforcement. On March 15, 2018, a grand jury in the Southern District of California indicted Defendant on charges of Racketeering Conspiracy and Conspiracy to Aid and Abet the Distribution of Cocaine in violation of 18 U.S.C. § 1962(d) and 21 U.S.C. § 981, respectively. On October 2, 2018, Defendant pleaded

guilty to the racketeering conspiracy. The United States recommends a sentence of 240 months in custody followed by five years of supervised release, and criminal forfeiture.

II.

STATEMENT OF THE CASE

Encrypted communications enable the expansion of transnational crime by permitting secure, global communications to be exchanged unimpeded and unmonitored by law enforcement despite lawful orders to do so. This technology permits the principals of criminal organizations to distance themselves from the reach of U.S. and foreign law enforcement while still allowing them to coordinate their criminal activities and access their "customers." Through secure communications, TCOs can plan activities with reduced risk of having these actions disrupted by law enforcement. Defendant, through the operation of his company Phantom Secure, weaponized this technology by designing a device specifically intended to prevent law enforcement from actively monitoring the communications between members of TCOs, and retrieving the information from a seized device. PSR ¶ 5. Because of the direct involvement in the marketing and distribution of these devices to TCOs, as well as his direct role in destroying evidence through remote deletion of evidence, the sentence recommended by the United States is more than warranted.

A. The Phantom Secure Device Was Designed Specifically to Obstruct and Impede Law Enforcement

The Phantom Secure device was essentially a Blackberry handset that Defendant purchased from Blackberry. Unlike a standard Blackberry device, however, Phantom Secure and Defendant stripped most of the functionality from the device, including GPS navigation, camera, Internet access, and the microphone rendering it useless for any purpose other than sending and receiving encrypted communications within a closed loop of other Phantom Secure customers. PSR ¶ 6. In exchange for its services and devices, Phantom Secure charged approximately $2000 for a sixth month subscription, or roughly the equivalent of a top-of-line iPhone with premium data plans. PSR ¶ 21(b).

B. Phantom Secure Designed and Marketed Its Services Directly to Criminals

As part of its marketing, Phantom Secure offered the following key services to its criminal users: (1) it provided PGP encryption which completely impeded law enforcement's ability to intercept criminal communications, and (2) it remotely erased devices if and when individual devices were seized by law enforcement. Defendant was personally involved in the development and marketing of these two core functionalities. He personally lauded Phantom Secure's products as impervious to decryption, wiretapping, or third-party records requests. He also guaranteed the destruction of evidence contained within a device if it fell into the hands of law enforcement and the organization notified Phantom Secure. Plea Agreement at II.B.4; PSR ¶ 5. This guarantee was not an empty promise; Phantom Secure routinely deleted and destroyed evidence from devices that it knew had been seized by law enforcement. Plea Agreement at II.B.9. Finally, as an extra layer of protection, the encrypted communications were routed through servers located in Panama and Hong Kong, a feature Phantom advertised as outside the reach of global law enforcement. PSR ¶ 6.

Internally, the company and Defendant also went to great lengths to protect its customers' anonymity and privacy by using code words like "executives" to describe individuals Defendant knew were involved in drug trafficking. Phantom Secure also refused to track or record its customers' real names and addresses. Phantom Secure also did not sell its product directly to the public, instead relying on a vouching system to develop new customers from its existing criminal customer base. Plea Agreement at II.B.6-8. Phantom Secure spread from customer to customer, criminal to criminal, TCO to TCO through word of mouth and an elaborate vouching system. PSR ¶ 8, 21(b).

Further, to ensure that law enforcement did not learn more about its services and devices, the company suspended service and deleted the contents of devices if it suspected it was being used by law enforcement or an informant. Plea Agreement at II.B.9.

C. Phantom Secure's Customer Base Was Comprised of Criminals

Conservatively, Phantom Secure had between 7,000 and 10,000 customers. PSR ¶ 7. To date, neither Australian, Canadian, nor American law enforcement has identified a single non-criminal user of Phantom Secure devices. Law enforcement has identified numerous criminal users, including at least one user who appeared before this court, Owen Hanson. Hanson's organization used approximately six Phantom Secure devices[1] to coordinate and ship more than a ton of cocaine from Mexico into Southern California and on to Canada and Australia. On December 15, 2017, this Court sentenced Owen Hanson to 255 months in custody for drug trafficking, money laundering, and running an illegal gambling organization. *See U.S. v. Owen Hanson,* 15CR2310-WQH.

Owen Hanson was not the only individual to use Phantom Secure devices to coordinate criminal activities. Phantom Secure devices have been used to coordinate drug trafficking and money laundering on a global scale. This fact was not a secret to Defendant as he explained to an RCMP agent before he was arrested by the FBI: "a lot of these guys [his customers] are dead or in jail."

Phantom Secure devices have also been used to coordinate violence, including murder. For example, the Hells Angels used Phantom Secure devices to coordinate several high profile murders in Australia. *See* March 5, 2014 ABC News article entitled "Uncrackable phones provided by Phantom Secure to murder of Hells Angels bikies" attached as Exhibit 1. While ABC specifically noted in its article that "it does not suggest the company itself is aware its products are being used by criminals," this Court need not accept this qualifier. The record is clear that not only was Defendant aware of this article and the underlying facts, he shockingly bragged about Phantom Secure's role, and used the "uncrackable" description as a marketing tool. In an internal memo stored on his Phantom device entitled "Aus ABC News," Defendant wrote, "this is the

[1] The devices appear to have been used by individuals in Mexico, Los Angeles, San Diego, Chicago, and New York City/New Jersey.

best verification on what we have been saying all along – proven and effective for now over 9 years. It is the highest level of official authority confirming our effectiveness. It can't get better than that." *See* Exhibit 2.

Phantom Secure allowed its customers to choose their own handles. Their choices are illustrative of the true makeup and nature of how they used Phantom Secure devices. For example, on Defendant's own device, "pabloescobar@cripticol.com" and "drugsbythekeys@secretmail.mobi" were listed as contacts. *See* Exhibits 3 and 4. The following are also a sample of the handles chosen by Phantom Secure's customers:

a. *leadslinger@freedomsecure.me*
b. *The.cartel@freedomsecure.me*
c. *The.killa@freedomsecure.me*
d. *narco@lockedpgp.com*
e. *Trigger-happy@lockedpgp.com*
f. *Knee_capper9@lockedpgp.com*
g. *Elchapo66@lockedpgp.com*
h. *Time4a187@freedomsecure.me*

D. The Defendant Was Directly Involved and Aware of Phantom Secure's Operations

Defendant was the undisputed leader of Phantom Secure as the CEO and founder. Plea Agreement at II.B.15; PSR ¶ 9. He started the company in 2008 for the specific purpose of selling a product that could "prevent law enforcement from actively monitoring the communications between members of transnational criminal organization." PSR ¶ 5. As the CEO, he could initiate new subscriptions, remove accounts, authorize remote deletions, and turn off devices. PSR ¶ 17. He controlled all of Phantom Secure's operations both directly and through the delegation of duties to others. PSR ¶ 9. He had decision-making authority of the administrators, distributors, and agents operating throughout the world. Plea Agreement at II.B.15. He set the policies and the price, dictated the range of services Phantom Secure provided, and was ultimately responsible for how the company operated.

Defendant's criminal culpability does not arise merely from the fact that he had the title CEO. Defendant was fully aware that his company's devices were used by criminals, and that Phantom Secure facilitated criminal acts and obstructed justice. First, Defendant was directly involved in marketing the device to TCOs. Second, Defendant used coded language to refer to his clients (e.g. "executives"), and repeatedly referred to law enforcement as "unfriendlies." Third, Defendant was directly aware that Phantom Secure destroyed evidence by wiping of devices seized by law enforcement.

In February 2018, Defendant travelled to Mexico City to market Phantom Secure devices to potential customers there. Before returning to Canada, Defendant visited Las Vegas where he communicated via text message with Phantom Secure employee. Within that text message, Defendant wrote, "we are fucking rich man I swear to go [sic] you better fucking appreciate it .. get the fucking Range Rover brand new. Cuz I just closed a lot of business. This week man. Sinaloa Cartel that's what up …". *See* Exhibit 5.

The substance and tone is corroborated by numerous memos found on Defendant's Phantom Secure device. For example, Defendant in a memo entitled "Password Conversation," Defendant wrote "Remember we are the leader in the industry and we spend money on research and consulting….we know that PGP is solid and works and the only way to get into a device is by brute force attack on the password." Defendant continued, "[t]he unfriendlies will send the device to a lab…[and] dump the memory with some forensic tools" and use "bruteforce attacks" to crack the password. Once the password has been circumvented, the "device full of secrets is now full of potential information that you did not want exposed!" It is clear that Defendant is referring to law enforcement. To eliminate any ambiguity, Defendant continued, "[o]h this is real life stuff my friend. I just read a [sic] indictment and the guy was using password *qwertypp*. Took them 1 month to crack it maybe even less. You want to be the most serious guy out there with the most serious reputation!" *See* Exhibit 6.

Defendant was personally aware that Phantom Secure remotely erased devices if they were seized by law enforcement. For example, on a February 28, 2018 email, Defendant was cc'ed[2] on a Phantom Secure message from Phantom Secure tech support that requested an immediate remote deletion because the device has been seized by law enforcement. The email, which contained the subject heading "Authorize Remote Wipe," continued, "Dear Distributor, Please confirm asap as user's contact person telling that it is with cops and need to be wiped without any delays." *See* Exhibit 7. In another unrelated exchange with a Phantom Secure distributor, Defendant noted that "[an] undercover asked my worker to wipe a berry and my worker said no. And then the undercover said…Hey wipe it pls because the pigs have it and we just brought in a load…My worker ended up wiping the device and they tried to get him for obstruction of justice..He got off but cost a lot in lawyer fees. So word of advice..Never ever acknowledge anything illegal." *See* Exhibit 8.

Finally, Defendant was personally involved in discussions with Phantom Secure customers and distributors about the potential that Phantom Secure distributors could work for law enforcement. In August 10, 2017 Phantom Secure message initiated by an individual calling himself "Vietnamese mafia" to another individual calling himself "Drug-syndicate," "Vietnamese mafia" stated there is a strong rumour that Bosspgp sales apparently been working with police and give out location and details of his clients. A few of my mates friends got pulled in. I wiped over 8 acc[ounts] today coz they had dealings with boss pgp emails. Spread word to ur boys whoever been dealing with boss pgp should be wiping their acc[ount]s." *See* Exhibit 9. This exchange was forwarded to Defendant who responded, "Yes..Hear all sorts of rumors. But I also know Bosspgp is one of Summers direct solid compliant guys. Authorities one day will ask you to cooperate to help them. But not like you will..Same type of thing." *Id*.

[2] Defendant's Phantom Secure handle was "Busi" or "Business."

III.

ARGUMENT

A. Guidelines Range

The parties have agreed to jointly recommend the following Base Offense Level and Adjustment:

1.	Base Offense Level (USSG § 2E1.1(a)(2)) (USSG § 2D1.1(c)(1))	38
2.	Aggravating Role (Organizer and Leader) (USSG § 3B1.1(a))	+4
4.	Acceptance of Responsibility (USSG § 3E1.1)	-3

These calculations yield a final adjusted offense level of 39, and with a Criminal History Category of I, Defendant falls within Zone D. This results in an advisory guidelines range of 262 to 327 in custody. Because Defendant pleaded to the RICO conspiracy, the statutory maximum sentence is 20 years or 240 months.

C. Sentencing Factors

1. Defendant Specifically Designed Phantom Secure to Facilitate Global Drug Trafficking

As the PSR makes clear, "the objectives of the Phantom Secure Enterprise were vast and troubling, including but not limited to maintaining a method of secure communication to facilitate the importation, exportation, and distribution of illegal drugs into Australia, Asia, Europe and North American, and laundering of proceeds of such drug trafficking conduct; as well as obstruct investigation of drug trafficking and money laundering organizations by maintaining a system whereby Phantom Secure could remotely delete evidence of such activities." PSR ¶ 110. In doing so, Defendant "created a harm to this country, as well as many other countries" in a way "that we likely not seen before." PSR ¶ 121.

Defendant specifically designed a product for and offered services to criminal organizations to facilitate the coordination of global drug trafficking. On the rare occasions when law enforcement successfully obtained a device that contained evidence of these crimes, Defendant's company destroyed that evidence from thousands of miles away. In providing these services, Defendant enriched himself, generating tens of millions of dollars in revenue, and personally accumulating a net worth of at least $10 million.

Even where the consequences of Phantom Secure's operation was not intentional, it was foreseeable to Defendant that his devices would enable thousands of criminals to commit crimes. As noted above, Owen Hanson used Phantom Secure devices to coordinate the transportation of more than a ton of cocaine from Mexico to Canada and Australia. Hanson used only six devices. Assuming the most conservative estimate of 7,000 Phantom Secure users, and extrapolating from Hanson's crimes, the number of crimes Phantom Secure facilitated is incalculable, and the amount of drugs "his company aided and abetted in transporting by providing devices and services to criminals worldwide was too high to calculate." PSR ¶ 121. Thus, given the massive quantities of drugs imported, exported, and distributed using Phantom Secure devices, Defendant's criminal acts generated clear and continuing risks to public health, and his sentence should reflect it.

2. Defendant Appears to Minimize His Role

And yet, Defendant appears to characterize his role in the spread of encryption, and Phantom Secure devices specifically, within the criminal underworld as a happenstance. To probation, Defendant claimed that he was generally unaware that criminals were using Phantom Secure devices, that when he "finally did become aware that in some instances is phones were being acquired by members of the drug world" he "should have [then] instituted rigorous background checks for all potential buyers." PSR ¶ 31. Probation specifically noted its concern that "RAMOS appeared to somewhat minimize his conduct in the instant offense" and appeared to be "intentionally pleading

ignorance" of how his actions led to "the activities his company and codefendant participated in over the last ten years." PSR ¶ 118.

Defendant's minimization of his role and understanding of company's operations and its customer base is undercut by the evidence available here. Months before he was arrested, Defendant travelled to Mexico City to develop business from the Sinaloa cartel. Defendant and his company (1) placed servers in Panama and Hong Kong to stay outside the reach of United State law enforcement, (2) required a personal reference (i.e. a vouch) from existing clients before selling a device and its service to a new customer, (3) employed code words to describe clients it knew or had reason to know were criminals, (4) deleted devices that fell into the hands of law enforcement, (5) suspended service of devices obtained by law enforcement or suspected informants, and (6) used cryptocurrencies to protect the identities of its customers, and (7) described law enforcement as "unfriendlies." Defendant personally directed his employees and distributor to not assist law enforcement, and to feign ignorance out the true nature of his customers' activities. His customers adopted handles like *leadslinger, thecartel, knee_capper,* and *Time4a187*. And perhaps most concerning, he used a gangland murder as a marketing opportunity for his product's imperviousness. These deliberate acts belie the notion that he intended his service for business executives seeking extra privacy.

Finally, Defendant's claims that he did not intend to create a product that would be used by career criminal and TCO's simply defies common sense. The marketplace is saturated with encrypted communications services and applications that can be downloaded onto an existing devices for *free*. It defies reason that individuals would pay $2,000 for a six-month subscription for a service that provides nothing more than what is commercially available for free unless those customers are really buying something else. Here, it is clear from the record criminals around the world were paying a premium for the assurance that they were dealing with a company and individuals that shared a common goals: (1) impeding law enforcement from executing its lawful

function of investigating and prosecuting criminal activity; and (2) facilitating organized crime.

3. Promote Respect for the Law and Deterrence

As stated by former FBI Director James Comey, "Encryption isn't just a technical feature; it's a marketing pitch. Sophisticated criminals will come to count on these means of evading detection. It's the equivalent of a closet that can't be opened. A safe that can't be cracked." Because "dark communication" represents an emerging front in the fight against crime, general deterrence interests are particularly salient sentencing factor in this case. In Defendant's own words, Phantom Secure was a "leader in the industry," and his sentencing is being closely monitored by TCOs and Phantom Secure's former competitors. After Phantom Secure was dismantled, Phantom Secure's competitors – undeterred by Defendant's experience – immediately absorbed nearly its entire customer base.

Thus, although Defendant is the first individual to be prosecuted by the United States government for this type of crime, he likely will not be the last. The Court has an opportunity to send a clear message to anyone tempted to follow his example that the operation of these illegal enterprises comes with severe consequences.

CONCLUSION

Given the enormous quantities of drugs criminals drug traffickers transported by using Phantom Secure devices, in combination with other aggravating factors, the United States recommends a custodial sentence of 240 months followed by a five years of supervised release, and forfeiture.

DATED: May 21, 2019

Respectfully submitted,

ROBERT S. BREWER, JR.
United States Attorney

/s/ Andrew P. Young
ANDREW P. YOUNG
BENJAMIN J. KATZ

ABC NEWS

Uncrackable phones provided by Phantom Secure linked to murder of Hells Angels bikies

7.30 By Dylan Welch

Updated Wed 5 Mar 2014, 12:11pm

Australian law enforcement agencies are increasingly unable to monitor the communications of some of the country's most powerful criminals due to the rising prevalence of uncrackable encrypted phones.

The phones are linked to a series of the underworld killings that rocked Sydney, several senior law enforcement officials told the ABC on condition of anonymity.

The phones are sold by dozens of companies worldwide and have legitimate uses.

But the law enforcement officials say thousands of the phones have been obtained by Australian criminals and they are using them to commit serious crimes, including murder.

One company is Phantom Secure, a Canadian-based seller of encrypted Blackberries.

PHOTO: Encrypted BlackBerry phones come at a cost of around $2,760. (AFP)

RELATED STORY: Dead bikie's family appeals for info on killer

RELATED STORY: Sydney shooting victims targeted in deliberate hit

The ABC does not suggest the company itself is aware its products are being used by criminals, only that criminals have become aware of the phone's utility and have taken advantage.

Phantom Secure did not respond to requests for an interview or to questions sent by the ABC.

The Phantom Blackberries cost up to $2,760, which includes a six-month subscription to the company's data service.

At the end of that subscription a user can spend a further $2,000 to renew their six-month subscription.

The Phantom phones have the microphone and camera removed and cannot be used to surf the web, send emails or texts or make calls. The only thing they can do is send messages using a private messaging system.

That system is protected by military-grade encryption and cannot be hacked even by Australia's electronic spy agency, the Australian Signals Directorate, said a Government official who declined to be named.

"Our intelligence would suggest that the most serious of crimes are being facilitated by... encrypted communications," Paul Jevtovic, the acting head of the Australian Crime Commission (ACC), said.

"We're talking about acts of violence; we're talking about a range of serious crime."

Phantom phone use suspected in hits on Hells Angels bikies

In particular, the ABC has learned that a well-known member of the Comanchero Motorcycle Club is suspected of ordering at least two high-profile killings in recent years using his encrypted Phantom Secure phone.

Those murders were of Tryone Slemnik, a newly minted Hells Angel member gunned down during a drive-by in Sydney's south in July last year, and Roy Yaghi, a Hells Angels associate and convicted drug cook who was shot dead in 2012 while sitting in a ute in Sydney's west.

NSW police are aware of a connection between the well-known Comancheros and the two killings, but have been stymied in their investigations due to the suspected use of the Phantom phone.

The ACC has launched several investigations into the use of encrypted communications and told the ABC the issue is a growing problem.

"Organised crime [has] seen that encrypted communications can allow them to plan and execute their criminal activities and prevents law enforcement detection. So clearly that's of concern to us; it has been for some time," Mr Jevtovic said.

"It's estimated that that in the next two years the [global encryption] market will double in size, which means there's a strong demand out there.

"Now whilst that demand is from legitimate industry and citizens who are not involved in crime, our concern is that organised crime will further avail themselves of this technology."

It's estimated that that in the next two years the [global encryption] market will double in size, which means there's a strong demand out there.

Paul Jevtovic

Two federal parliamentary committees recently recommended the Government undertake wholesale reform to the legislation that regulates how police and intelligence agencies can monitor people's phones, the 1978 Telecommunications (Interceptions and Access) Act, in the hope of clawing back some ground from criminals using the high-tech phones.

"The rapid uptake of new communication technologies and encryption by organised crime and terrorist groups is a significant concern and the Attorney-General's Department is currently pursuing reforms to the telecommunications interception legal framework," Justice Minister Michael Keenan said.

ASIO and the federal police declined to comment about the issue. The Australian Signals Directorate told the ABC they were aware of Phantom Secure but also turned down an interview.

Topics: murder-and-manslaughter, crime, law-crime-and-justice, crime-prevention, mobile-phones, information-and-communication, science-and-technology, sydney-2000, nsw, australia

First posted Wed 5 Mar 2014, 12:43am

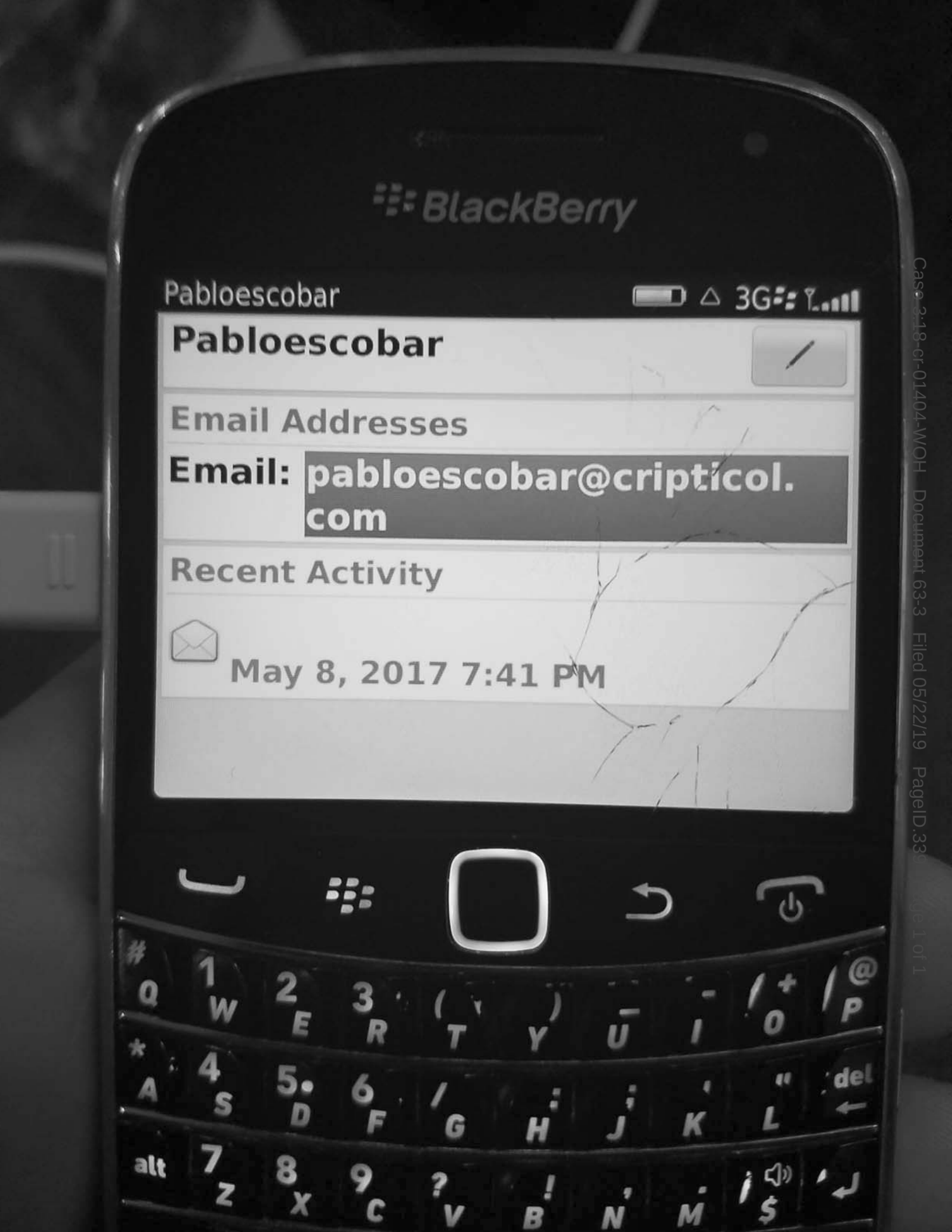
Edit Memo

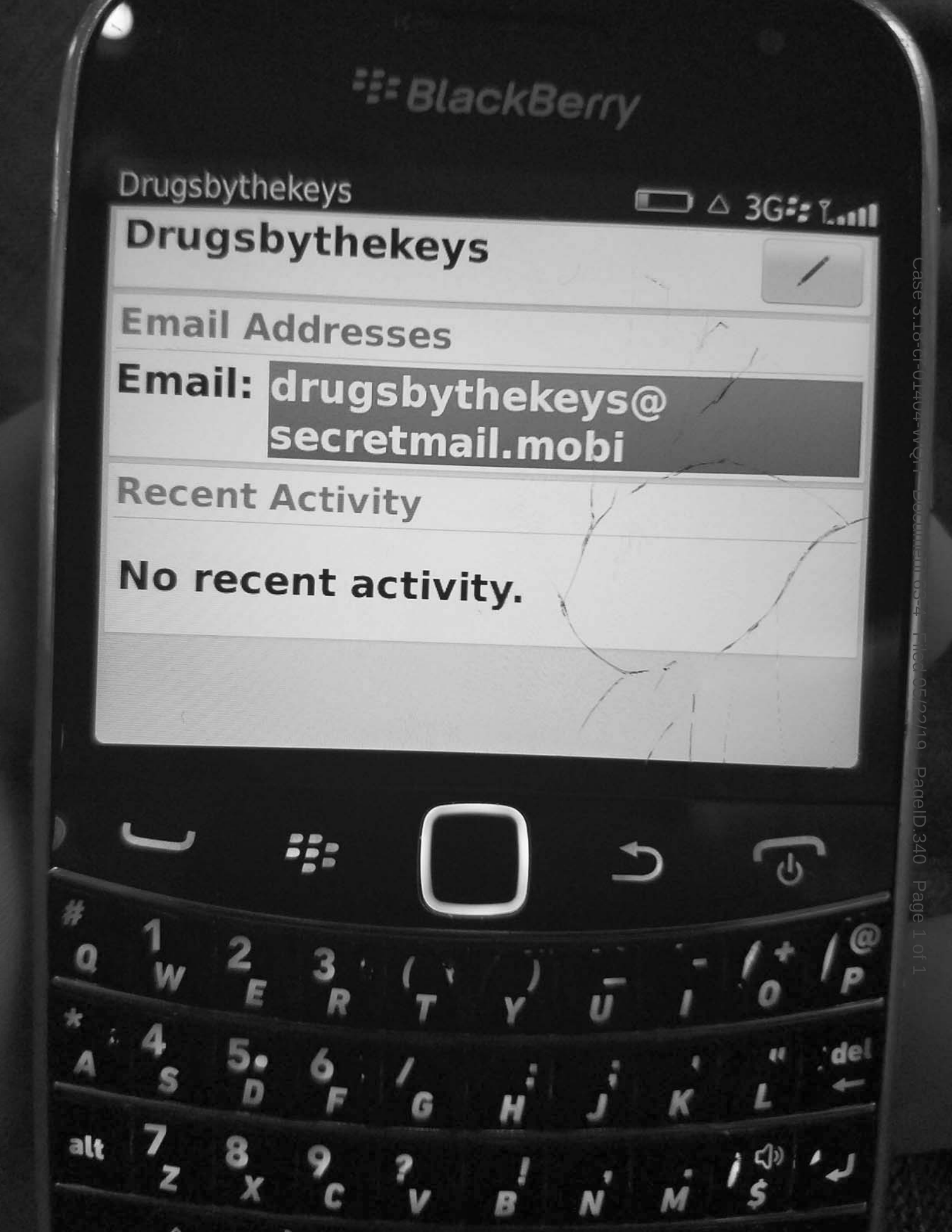
NL

Title: Aus ABC News

This is the best verification on what we have been saying all along - proven and effective for now over 9 years.

It is the highest level of official authority confirming our effectiveness. It can't get better than that.





12:03 AM 58%

[redacted]

Tap here for settings

Feb 7, 2018 5:47 PM

Guy Goes To Mexico To Kill Himself, Spends Week Doing Coke And Banging Hookers, Decides To Keep Living

Share Tweet Email Nice Move

Proud of you

Thanks bro. Lol.

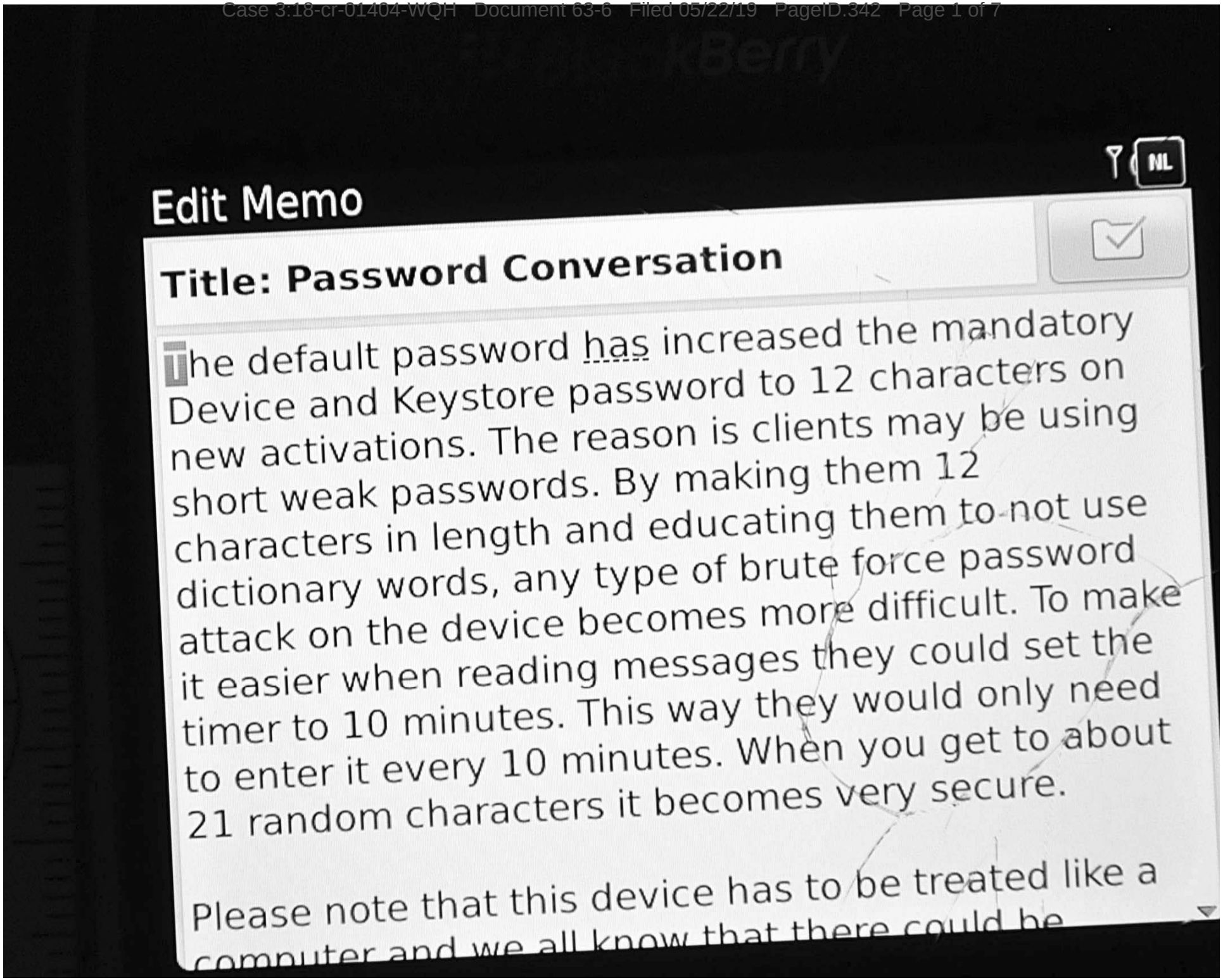
Feb 8, 2018 5:18 AM

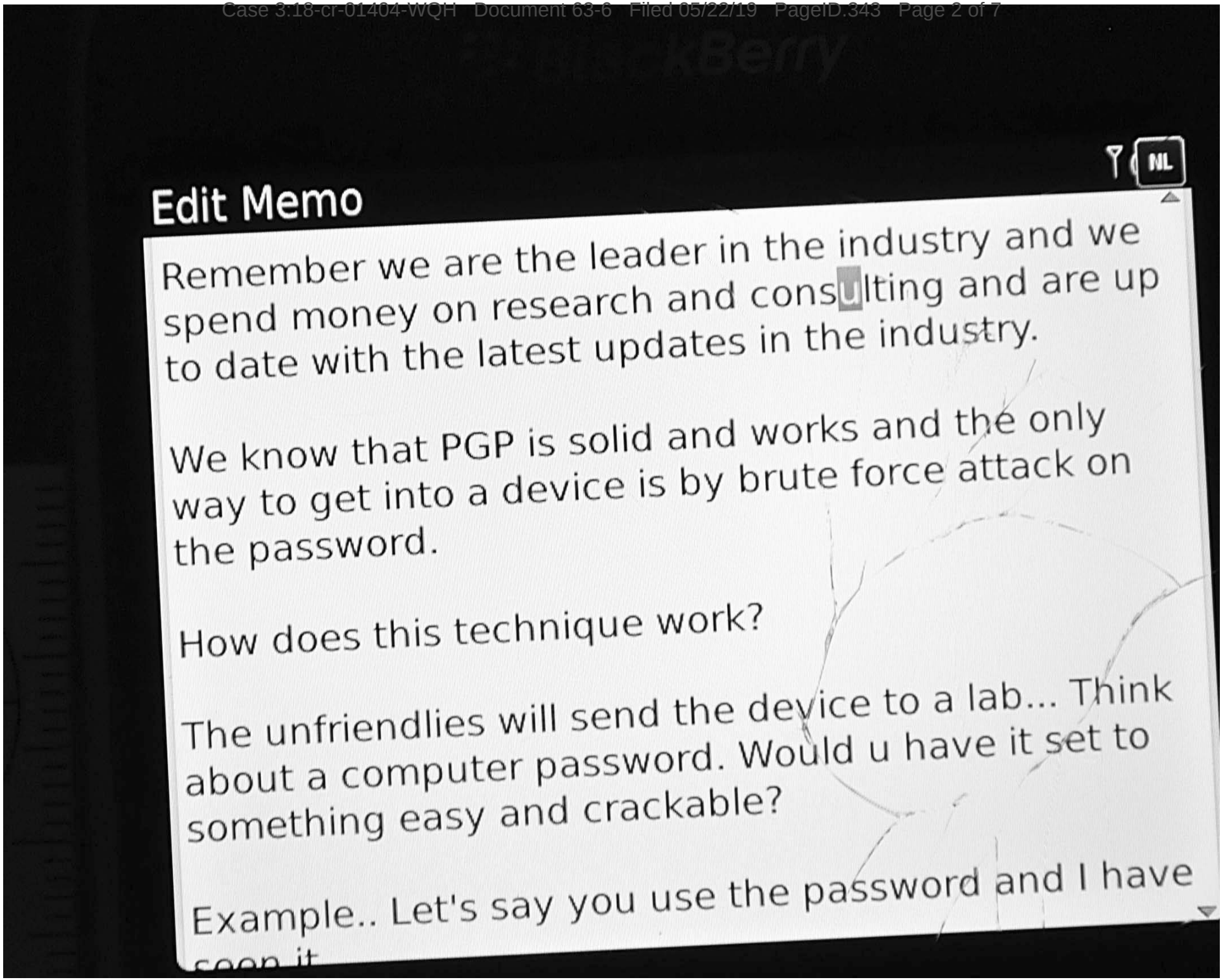
Still at rhino. I'm with Richard Sherman and some other black guys lol.. we are fucking rich man I swear to go you better fucking appreciate it.. get the fucking Range Rover brand new. Cuz I just cloSed a lot of business. This week man. Sinaloa Cartel that's what's up and my boy is Punjabi Cartel lol

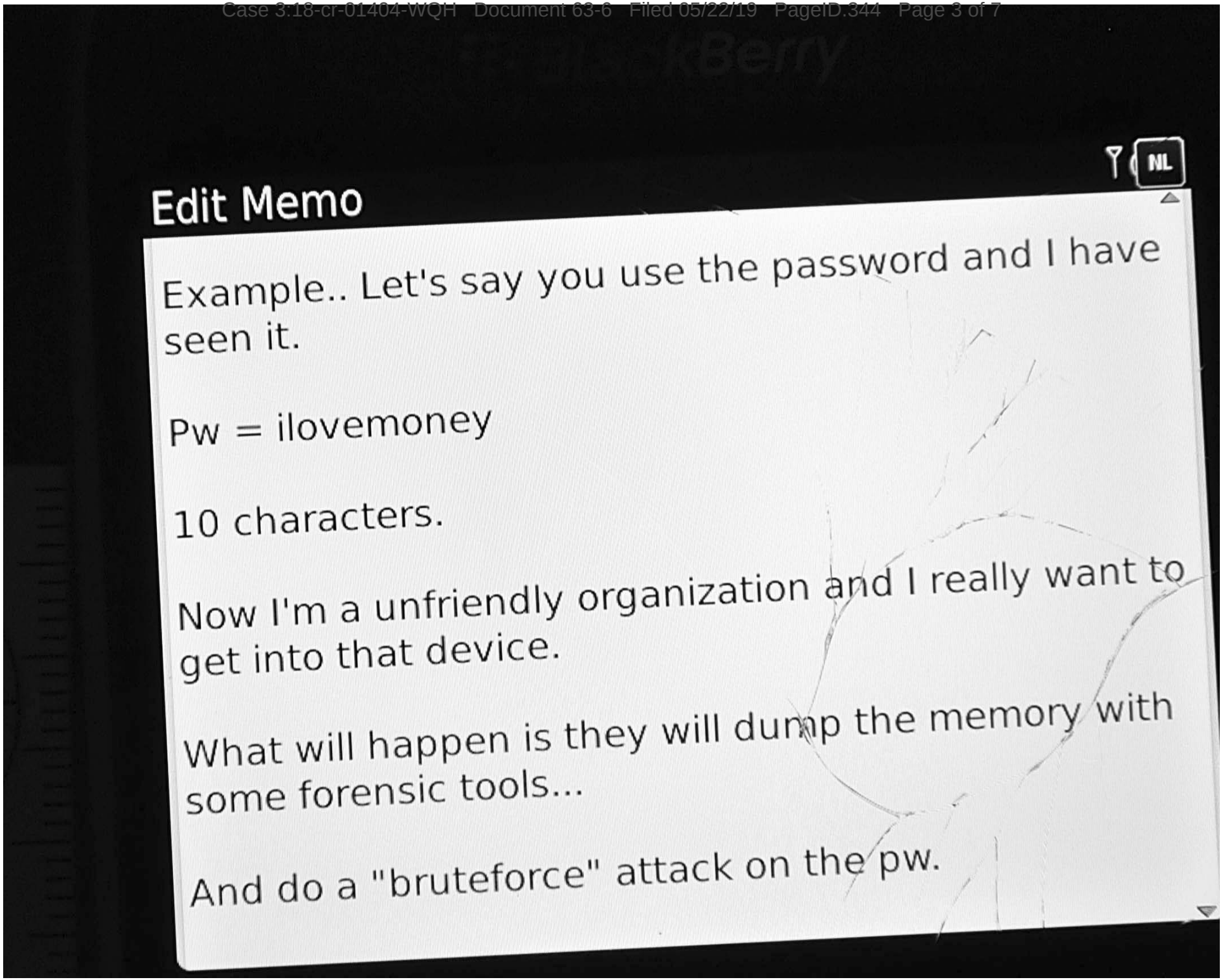
Straight u

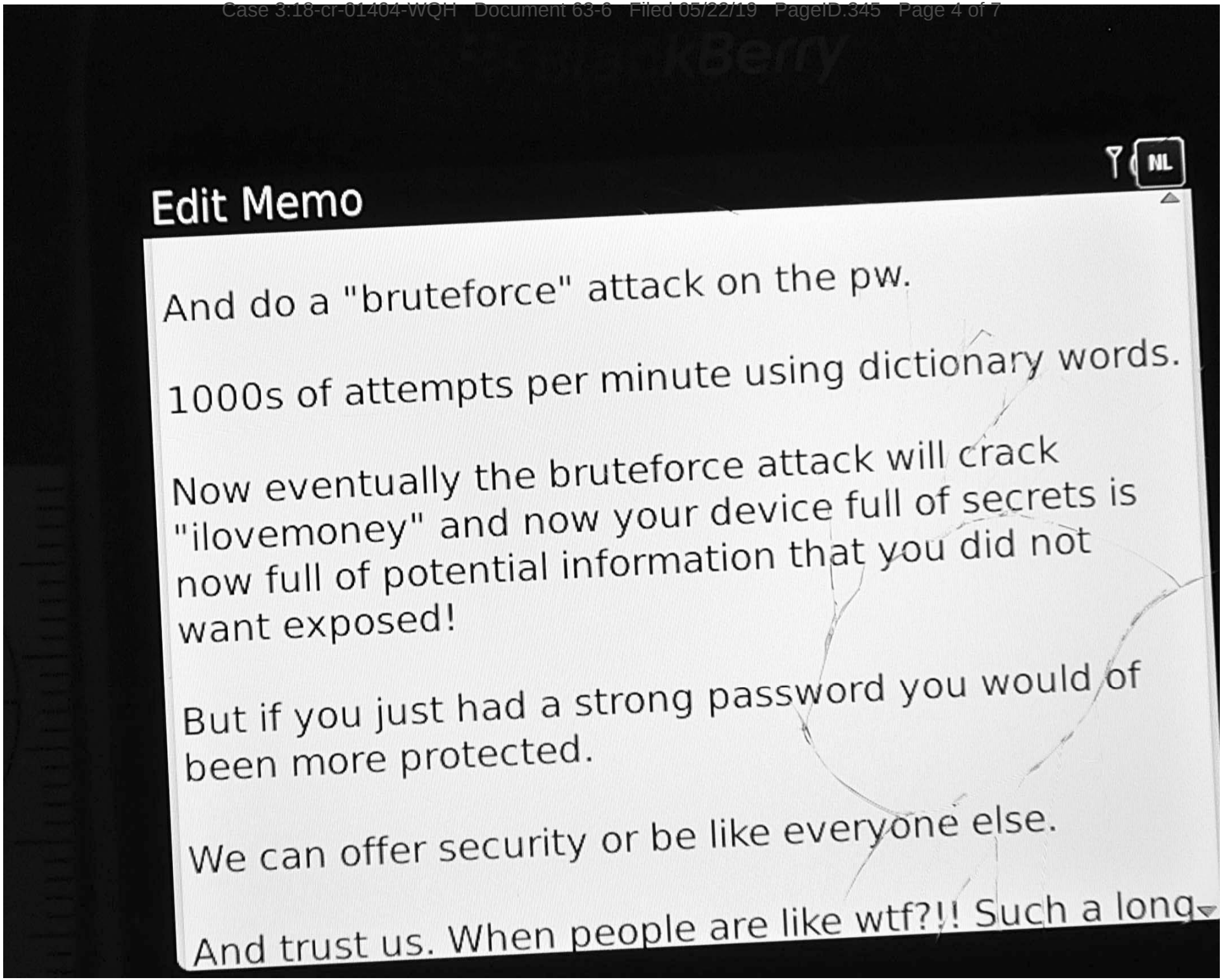
Feb 8, 2018 7:55 AM

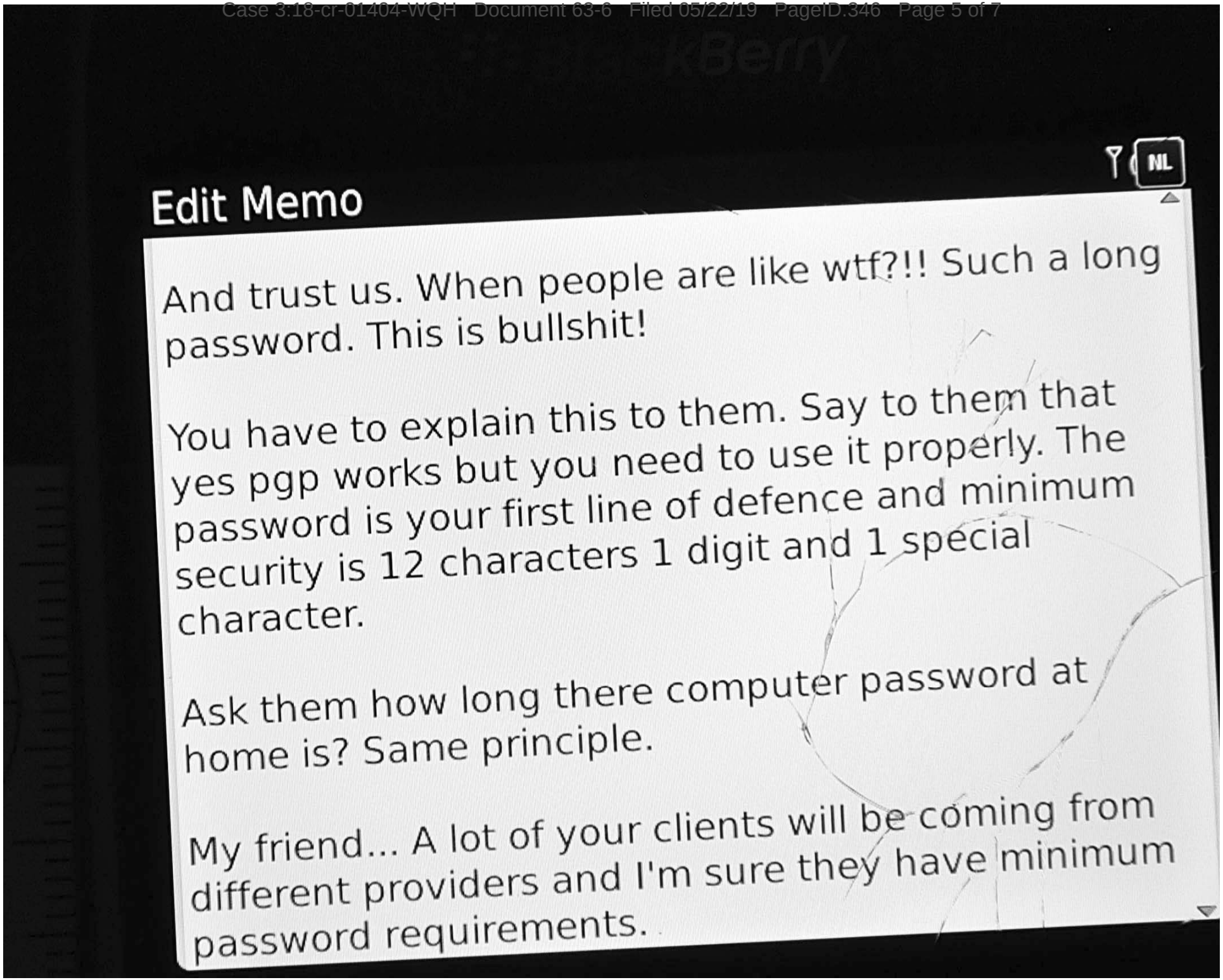
New Message

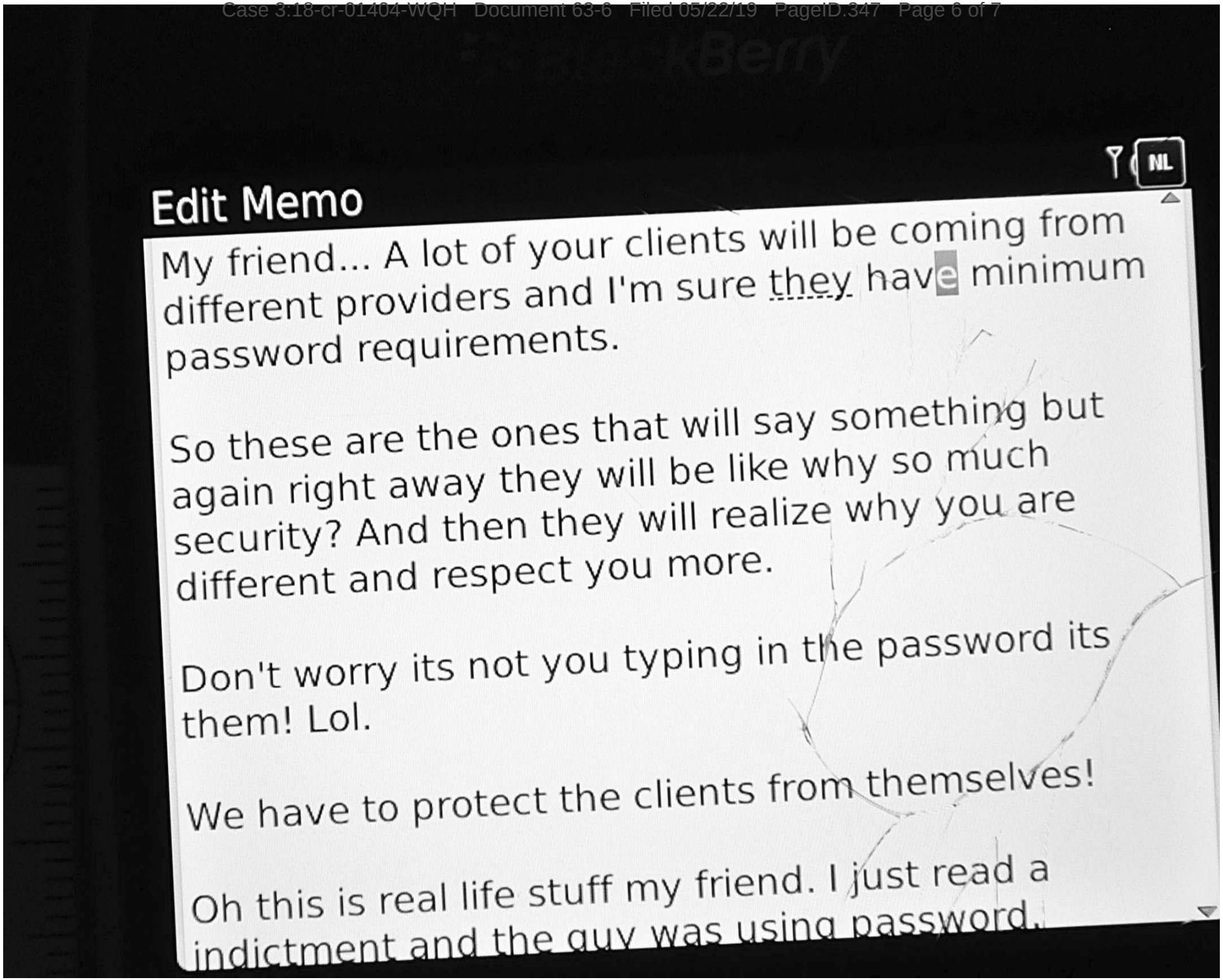

Edit Memo
Title: Password Conversation
The default password has increased the mandatory Device and Keystore password to 12 characters on new activations. The reason is clients may be using short weak passwords. By making them 12 characters in length and educating them to not use dictionary words, any type of brute force password attack on the device becomes more difficult. To make it easier when reading messages they could set the timer to 10 minutes. This way they would only need to enter it every 10 minutes. When you get to about 21 random characters it becomes very secure.
Please note that this device has to be treated like a

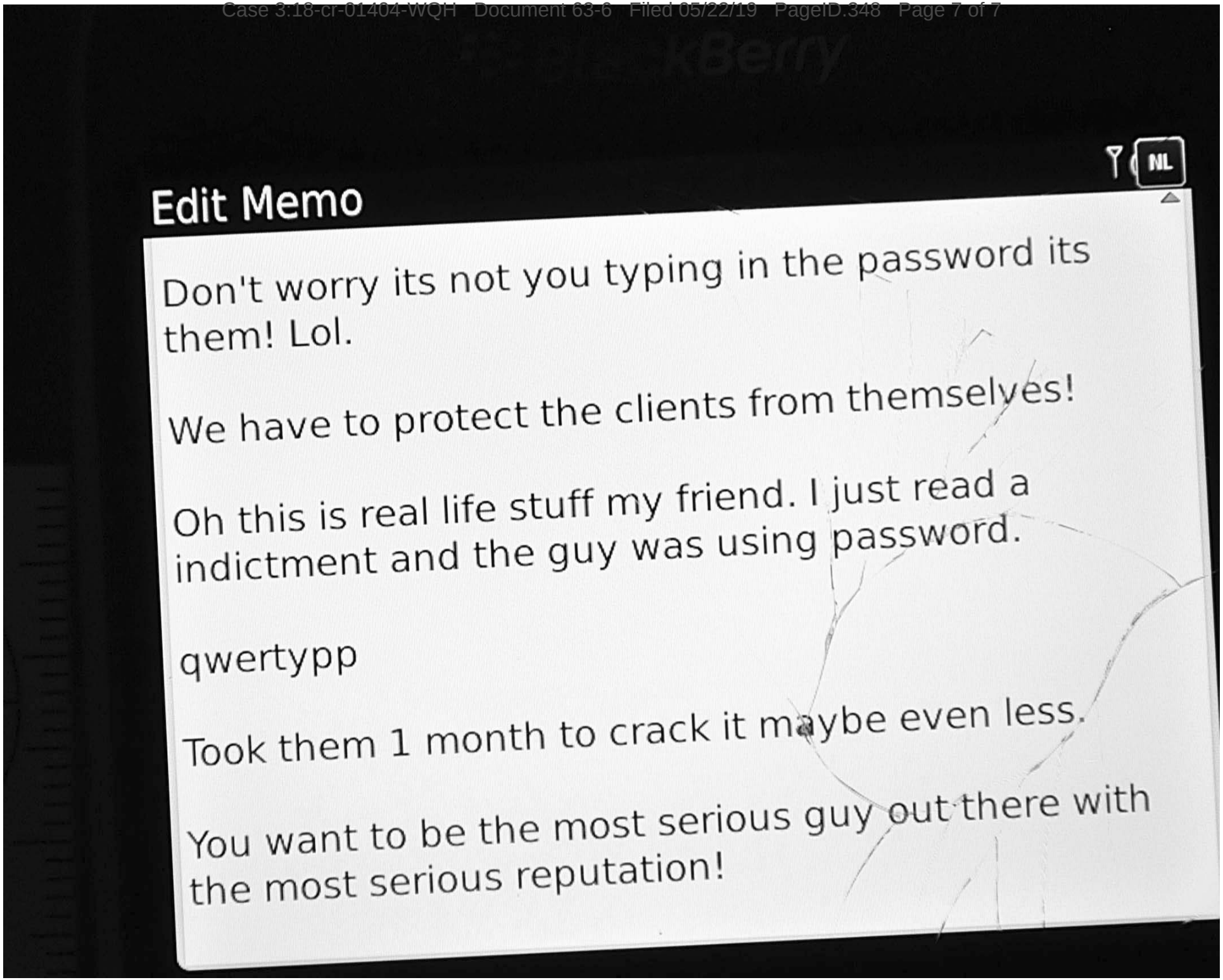

Edit Memo
NL
Remember we are the leader in the industry and we spend money on research and consulting and are up to date with the latest updates in the industry.
We know that PGP is solid and works and the only way to get into a device is by brute force attack on the password.
How does this technique work?
The unfriendlies will send the device to a lab... Think about a computer password. Would u have it set to something easy and crackable?
Example.. Let's say you use the password and I have


NL
Edit Memo
Example.. Let's say you use the password and I have seen it.
Pw = ilovemoney
10 characters.
Now I'm a unfriendly organization and I really want to get into that device.
What will happen is they will dump the memory with some forensic tools...
And do a "bruteforce" attack on the pw.

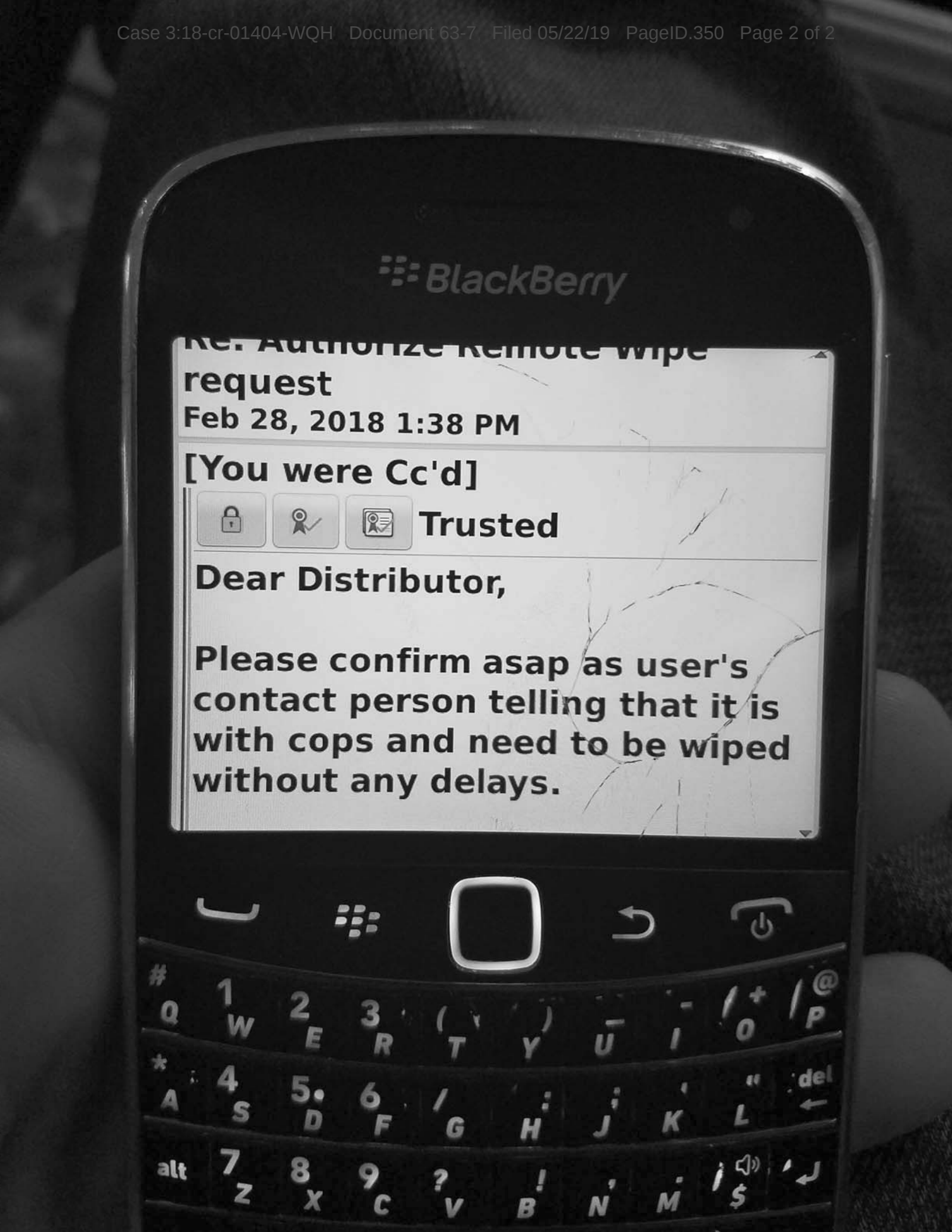

BlackBerry
NL
Edit Memo
And do a "bruteforce" attack on the pw.
1000s of attempts per minute using dictionary words.
Now eventually the bruteforce attack will crack "ilovemoney" and now your device full of secrets is now full of potential information that you did not want exposed!
But if you just had a strong password you would of been more protected.
We can offer security or be like everyone else.
And trust us. When people are like wtf?!! Such a long


NL
Edit Memo
And trust us. When people are like wtf?!! Such a long password. This is bullshit!
You have to explain this to them. Say to them that yes pgp works but you need to use it properly. The password is your first line of defence and minimum security is 12 characters 1 digit and 1 special character.
Ask them how long there computer password at home is? Same principle.
My friend... A lot of your clients will be coming from different providers and I'm sure they have minimum password requirements.


Edit Memo
NL
My friend... A lot of your clients will be coming from different providers and I'm sure they have minimum password requirements.
So these are the ones that will say something but again right away they will be like why so much security? And then they will realize why you are different and respect you more.
Don't worry its not you typing in the password its them! Lol.
We have to protect the clients from themselves!
Oh this is real life stuff my friend. I just read a indictment and the guy was using password.


Edit Memo
NL
Don't worry its not you typing in the password its them! Lol.
We have to protect the clients from themselves!
Oh this is real life stuff my friend. I just read a indictment and the guy was using password.
qwertypp
Took them 1 month to crack it maybe even less.
You want to be the most serious guy out there with the most serious reputation!


BlackBerry
Importance: High
Sensitivity: Private
To: 'i.support@knoxsecure.glob...
To: Businessmind BM
Cc: CS
Cc: Busi
From: Tech pscom
Re: Authorize Remote Wipe request
Feb 28, 2018 1:38 PM
[You were Cc'd]


BlackBerry
request
Feb 28, 2018 1:38 PM
[You were Cc'd]
Trusted
Dear Distributor,
Please confirm asap as user's contact person telling that it is with cops and need to be wiped without any delays.

[redacted]

Encrypted

Lol.. Ya dont ask clients. No need to know

fyi... A undercover asked my worker to wipe a berry and my worker said no.

And then the undercover said..

Hey wipe it pls because the pigs have it and we just brought in a load..

My worker ended up wiping the device and they tried to get him for obstruction of justice.. He got off but cost a lot in lawyer fees.

So word of advice.. Never ever acknowledge anything illegal

PSB Of

business@phantomsecure.com

EDIT

Sent: Aug 10, 2017 10:28 AM

----Original Message----
From: Vietnamese mafia
To: Drug-syndicate
Subject: Important info
Sent: Aug 10, 2017 3:26 AM

Word of caution. There is a strong rumour that Bosspgp sales apparently
been working with police and give out location and details of his
clients. Afew of my mates friends got pulled in. I wiped over 8 accs
today coz they had dealings with boss pgp emails. Spread word to ur boys
whoever been dealing with boss pgp should be wiping their accs.

Best Regards,

Sales
Head of Sales and Distribution
E:Sales@solidcrypt.mobi
SOLIDCRYPT INC - Your No.1 Trusted PGP
BB Supplier

[redacted]

10 Aug 2017, 3:59 pm

Encrypted

Yes.. Hear all sorts of rumors.

But I also know. Bosspgp is one of Summers direct solid compliant guys. Authorities one day will ask you to cooperate to help them.

But not like you will.. Same type of thing

----Original Message----
From: [redacted]
To: Busi
Subject: Re:
Sent: Aug 9, 2017 10:52 PM

Just passing it on bro, you have heard this rumour before I take it?

On 10 August 2017 15:48:49 GMT+10:00, Phantom Secure Business <business@phantomsecure.com> wrote:
This is simply just a rumor.