SEKRETESS

Polisen

Tilläggsprotokoll

till 5000-K287846-25

Arkiv/Åkl. ex

Åklnr
AM-34865-25

Signerat av
FE7B-B8VU

Enhet
Polisregion Nord, Utredning 3 LPO Umeå

Handläggare (Protokollförare)
FE7B-B8VU

Undersökningsledare
Jenny Östling

Polisens diarienummer
5000-K287846-25

Personer i ärendet

Förtursmål	Beslag	Målsägande vill bli underrättad om tidpunkt för huvudförhandlingen
Annat förtursmål		Nej
Ersättningsyrkanden		Tolk krävs

Misstänkt (Efternamn och förnamn)	Personnummer
Johansson, Peter Kevin Leonard	20070921-2450

Brott	Förhandsgodkännande enligt RB 48:10
	Nej

Misstänkt har delgivits information om att förenklad delgivning kan komma att användas av polis och tingsrätt (skriftligt överlämnad vid ett personligt sammanträffande).

Misstänkt har delgivits information om att tillgänglighetsdelgivning kan komma att användas av tingsrätt (skriftligt överlämnad vid ett personligt sammanträffande).

Underrättad om slutförd förundersökning / utredning enligt RB 23:18a	Yttrande senast (rådrum)
2026-05-15, muntlig underrättelse	2026-05-15
	Resultat av slutunderrättelse: Ingen erinran

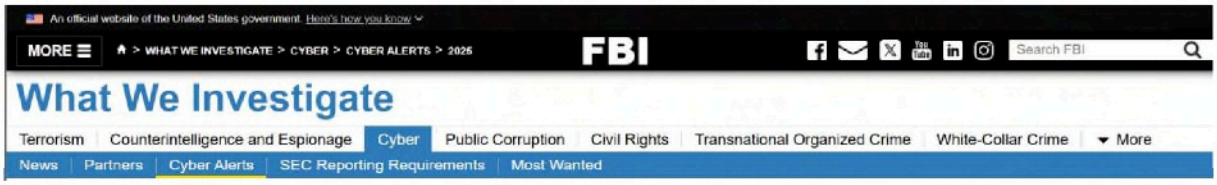
Försvarare
Töyrä, Emily, förordnad 2025-04-15

Underrättad om slutförd förundersökning / utredning	Yttrande senast (rådrum)
2026-05-15, muntlig underrättelse	2026-05-15
	Resultat av slutunderrättelse: Ingen erinran

Notering

Innehållsförteckning

Länk: https://www.fbi.gov/investigate/cyber/alerts/2025/violent-online-networks-target-vulnerable-and-underage-populations-across-the-united-states-and-around-the-globe



Public Service Announcement

Share on X X.com Share on Facebook Facebook Email Email

March 6, 2025

Violent Online Networks Target Vulnerable and Underage Populations Across the United States and Around the Globe

Alert Number: I-030625-PSA

Questions regarding this PSA should be directed to your local FBI field office.

The Federal Bureau of Investigation (FBI) is warning the public of a sharp increase in the activity of "764" and other violent online networks, which operate within the United States and around the globe. These networks methodically target and exploit minors and other vulnerable individuals, and it is imperative the public be made aware of the risk and the warning signs exhibited by victims.

These networks use threats, blackmail, and manipulation to coerce or extort victims into producing, sharing, or live-streaming acts of self-harm, animal cruelty, sexually explicit acts, and/or suicide. The footage is then circulated among members of the network to continue to extort victims and exert control over them.

Violent Online Networks

Some of the violent actors in these online networks are motivated by a desire to cause fear and chaos through their criminal conduct. However, motivations are highly individualized, and some threat actors may be engaging in criminal activity solely for sexual gratification, social status or a sense of belonging, or for a mix of other reasons that may not be ideologically motivated.

Targeting

These networks exist on publicly available online platforms, such as social media sites, gaming platforms, and mobile applications commonly used by young people. Many threat actors systematically target underage females, but anyone—juveniles, adults, males, and females—can be targeted. Victims are typically between the ages of 10 and 17 years old, but the FBI has seen some victims as young as 9 years old.

These violent actors target vulnerable populations, to include children as well as those who struggle with a variety of mental health issues, such as depression, eating disorders, or suicidal ideation. Threat actors often groom their victims by first establishing a trusting or romantic relationship before eventually manipulating and coercing them into engaging in escalating harmful behavior designed to shame and isolate them.

Extortion and Self-Harm

The networks use extortion and blackmail tactics, such as threatening to swat[1] or dox[2] their victims, if the victims do not comply with the network's demands. The actors can manipulate or coerce victims to produce child sexual abuse material (CSAM) and other videos depicting animal cruelty and self-harm. Self-harm activity can include cutting, stabbing, or fansigning.[3]

Members of the networks threaten to share the explicit videos or photos of the victims with the victims' family, friends, and/or post the photos and videos to the internet. The networks control their victims through extreme fear, and many members have an end-goal of forcing the victims they extort or coerce to live-stream their own suicide for the network's entertainment or the threat actor's own sense of fame.

Recommendations

The FBI urges the public to exercise increased vigilance when posting personal photos, videos, or personal identifying information, or direct messaging online. Although seemingly innocuous when posted or shared, the images and videos can provide malicious actors an abundant supply of content to exploit and manipulate or alter for criminal activity. Victims are vulnerable to embarrassment, harassment, extortion, or continued long-term re-victimization. The FBI recommends looking for warning signs indicating a victim may be engaging in self-harm or having suicidal thoughts.

The FBI recommends that family, friends, and associates consider the following potential indicators and warning signs:

- Sudden behavior changes such as becoming withdrawn, moody, or irritable.
- Sudden changes in appearance, especially neglect of appearance.
- Changes in eating or sleeping habits.
- Dropping out of activities and becoming more isolated and withdrawn.
- A new online "friend" or network prospective victims seem infatuated with and/or scared of.
- Receipt of anonymous gifts, such as items delivered to your home, currency, gaming currency or other virtual items.
- Scars, often in patterns.
- Fresh cuts, scratches, bruises, bite marks, burns, or other wounds.
- Carvings, such as words or symbols, on the skin.
- Wearing long sleeves or pants in hot weather.
- Writing in blood or what appears to be blood.
- Threatening to commit suicide and openly talking about death, not being wanted or needed, or not being around.
- Idealization of mass shooting or mass casualty events.
- Family pets or other animals being harmed or dying under suspicious circumstances.
- Family pets uncharacteristically avoid or are fearful of your child or you.
- Law enforcement being called to the home under false pretenses (known as swatted or doxxed) by an unknown person.

The FBI recommends the public consider the following when sharing content (e.g., photos and videos) or engaging with individuals online:

- Monitor children's and other vulnerable individuals' online activity and discuss risks associated with sharing personal information.
- Use discretion when posting images, videos, and personal content online, particularly those that include children or their information.

For more information on how to protect children and others refer to information on online risks here: Parents, Caregivers, Teachers—FBI.

Additional Resources

If you are worried about someone who might be self-harming or is at risk of suicide the following resources may help:

- Consult your pediatrician or other health care provider who can provide an initial evaluation or a referral to a mental health professional.
- Connecting your child to a mental health resource can help them learn healthy coping skills for intense emotions and help reduce the risk of a serious injury.
- If it is an immediate, life-threatening emergency dial 9-1-1.
- The National Center for Missing and Exploited Children provides a free service known as Take It Down, which helps minor victims—even if they are now an adult—remove or stop the online sharing of nude or sexually explicit online content. For more information, visit https://takeitdown.ncmec.org.

If you believe you are the victim of a crime using these tactics, retain all information regarding the incident (e.g., usernames, email addresses, websites or names of platforms used for communication, photos, videos, etc.) and immediately report it to:

- The FBI's Internet Crime Complaint Center at www.ic3.gov
- Your local FBI field office or 1-800-CALL-FBI (225-5324)
- National Center for Missing and Exploited Children (www.cybertipline.org or 1-800-THE LOST)

Reporting these crimes can help law enforcement identify malicious actors and prevent further victimization.

---

[1] Swat also referred to as swatting is the action or practice of making false emergency calls to police or other emergency services in an attempt to bring about the dispatch of armed police officers, such as a SWAT team, to a particular address.

[2] Dox, also referred to as doxxing, is the action of obtaining and publishing personally identifiable information (PII) on the internet, usually for malicious intent.

[3] Fansigning is writing or cutting specific numbers, letters, symbols, or names onto one's body.

Länk: https://www.fbi.gov/investigate/cyber/alerts/2025/in-real-life-com-violent-subset-of-the-community-is-a-rising-threat-to-youth-online

Public Service Announcement

Share on X X.com Share on Facebook Facebook Email Email

July 23, 2025

In Real Life (IRL) Com: Violent Subset of The Community (Com) is a Rising Threat to Youth Online

Alert Number: I-072325-2-PSA

Questions regarding this PSA should be directed to your local FBI field office.

The Federal Bureau of Investigation is warning the public about In Real Life (IRL) Com, one of three subsets of the growing and evolving online threat group known as The Com, short for The Community. The Com is a primarily English speaking, international, online ecosystem comprised of multiple interconnected networks whose members, many of whom are minors, engage in a variety of criminal violations. The members within IRL Com typically have a shared interest, ideology, or goal and work together, adding others to the group and splintering when necessary, to achieve their mission.

IRL Com, which initially stemmed from the subscriber identity module (SIM) swapping[1] community, includes subgroups that provide violence as a service (VaaS) and encompasses a range of violent crime. IRL services include shootings, kidnappings, armed robbery, stabbings, physical assault, and bricking. Services are posted online with a price breakdown for each act of violence. Groups offering VaaS advertise contracts on social media platforms to solicit individuals willing to conduct the act of violence for monetary compensation.

Much of the IRL violence within The Com arose from online conflicts in the SIM swapping community; however, the IRL violence has not only intensified but also expanded to other layers of The Com, emerging as its own market. IRL violence, or the threat of violence, is a tool to harass and intimidate targets. The spread of the VaaS market has led other layers of The Com to adopt similar methods of retaliation.

Swatting and In Real Life Com

IRL Com subgroups offer swat[2]-for-hire services via communication applications and social media platforms. Infighting among Com subgroups often leads to targeted swatting and doxing of members. IRL Com actors who offer these swatting services use platforms and technologies to obscure their true identities and are often paid in cryptocurrency.

The goal of swatting differs among The Com subgroups. IRL Com groups use swatting as a way to earn money. The IRL Com groups also see swatting as a way of gaining credibility among members; the more attention a swatting incident gets, the more attention the member receives from the group. Additionally, leaders from IRL Com groups may use swatting to ensure members of the group remain

obedient. When members of the IRL Com group disobey orders or refuse to comply with demands, the member or the member's family may become the target of swatting.

Victim Reporting and Additional Resources

If you or someone you know may be a victim of a crime using the tactics outlined above, the following resources may help:

- If it is an immediate, life-threatening emergency, dial 9-1-1.
- Consult a health care provider who can provide an initial evaluation or referral to a mental health professional.
- Connect to a mental health resource who can help with health coping skills for intense emotions and help reduce the risk of a serious injury.
- The National Center for Missing and Exploited Children (NCMEC) provides a free service known as Take It Down, which helps minor victims, or adults who were victimized as minors, with removing or stopping the online sharing of nude, or sexually explicit content taken while under 18 years old. For more information, visit takeitdown.ncmec.org.
- Contact your account providers immediately to regain control of your accounts, change passwords, and place alerts on your accounts for suspicious login attempts and/or transactions.
- Retain all of the information regarding the incident (i.e. usernames, email addresses, monikers, websites, platforms used for communication, names, photos, videos, etc.) and immediately report it to:
  - FBI's Internet Crime Complaint Center: ic3.gov
  - FBI field offices: fbi.gov/contact-us/field-offices or 1-800-CALL-FBI (225-5324)
  - National Center for Missing and Exploited Children (NCMEC): 1-800-THE-LOST or report.cybertip.org

---

[1] Subscriber identity module (SIM) swapping is a method in which a cyber criminal performs an unauthorized account takeover of a victim's wireless account held with the mobile phone carrier. This is accomplished by linking the victim's mobile phone number to a different SIM card within the same carrier's network but installed in a device the cyber criminal controls.

[2] Swattingis the act of reporting a false emergency situation with the intention of eliciting a law enforcement or SWAT response.

Resources

- The Com: Theft, Extortion, and Violence are a Rising Threat to Youth Online
- Hacker Com: Cyber Criminal Subset of The Community Is a Rising Threat to Youth Online

Polisen

Chatt gällande hässelby 1

Signerat av

Signerat datum

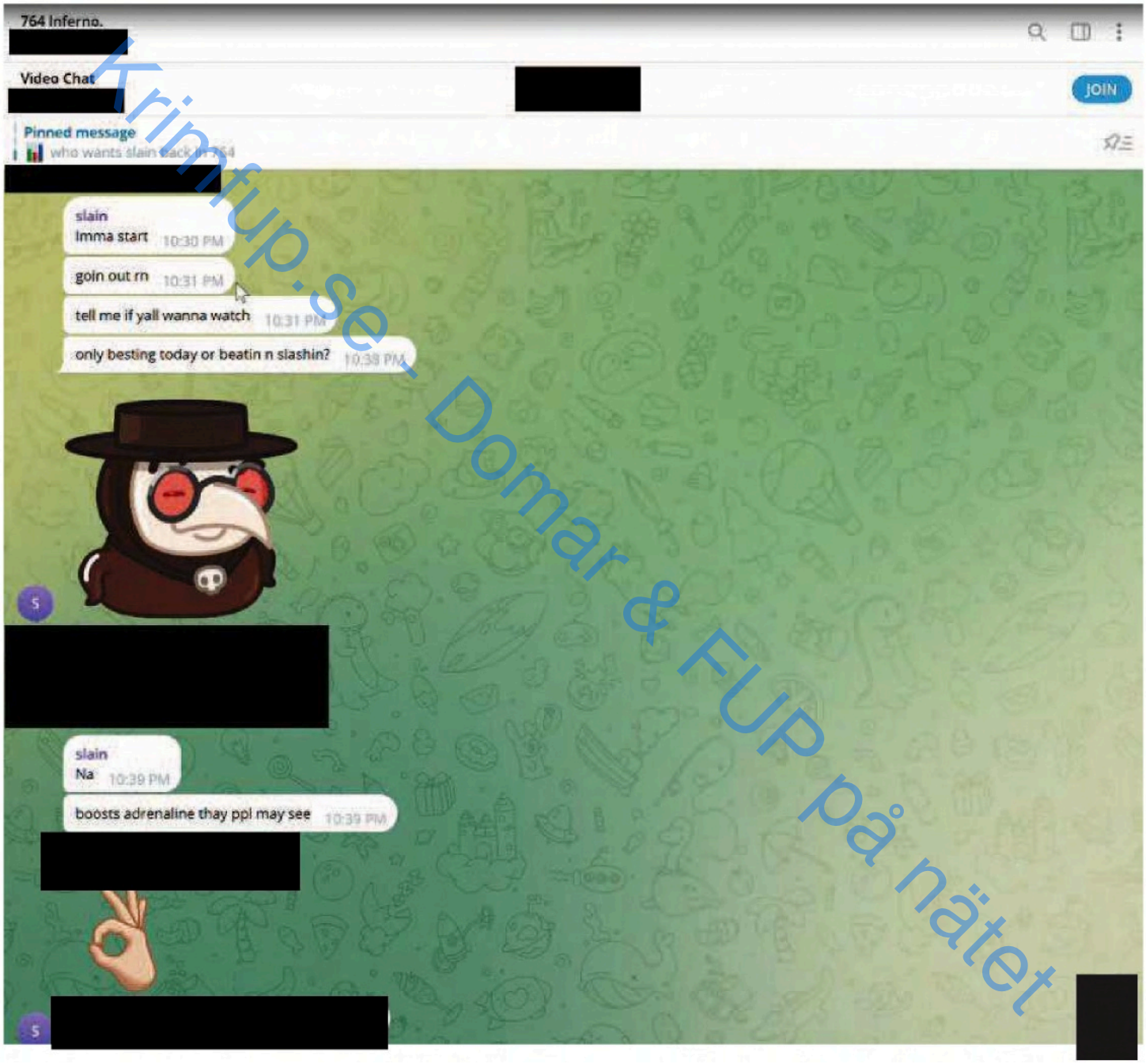
Enhet	Diarienr
Polisregion Nord, Utredning 3 LPO Umeå	5000-K287846-25

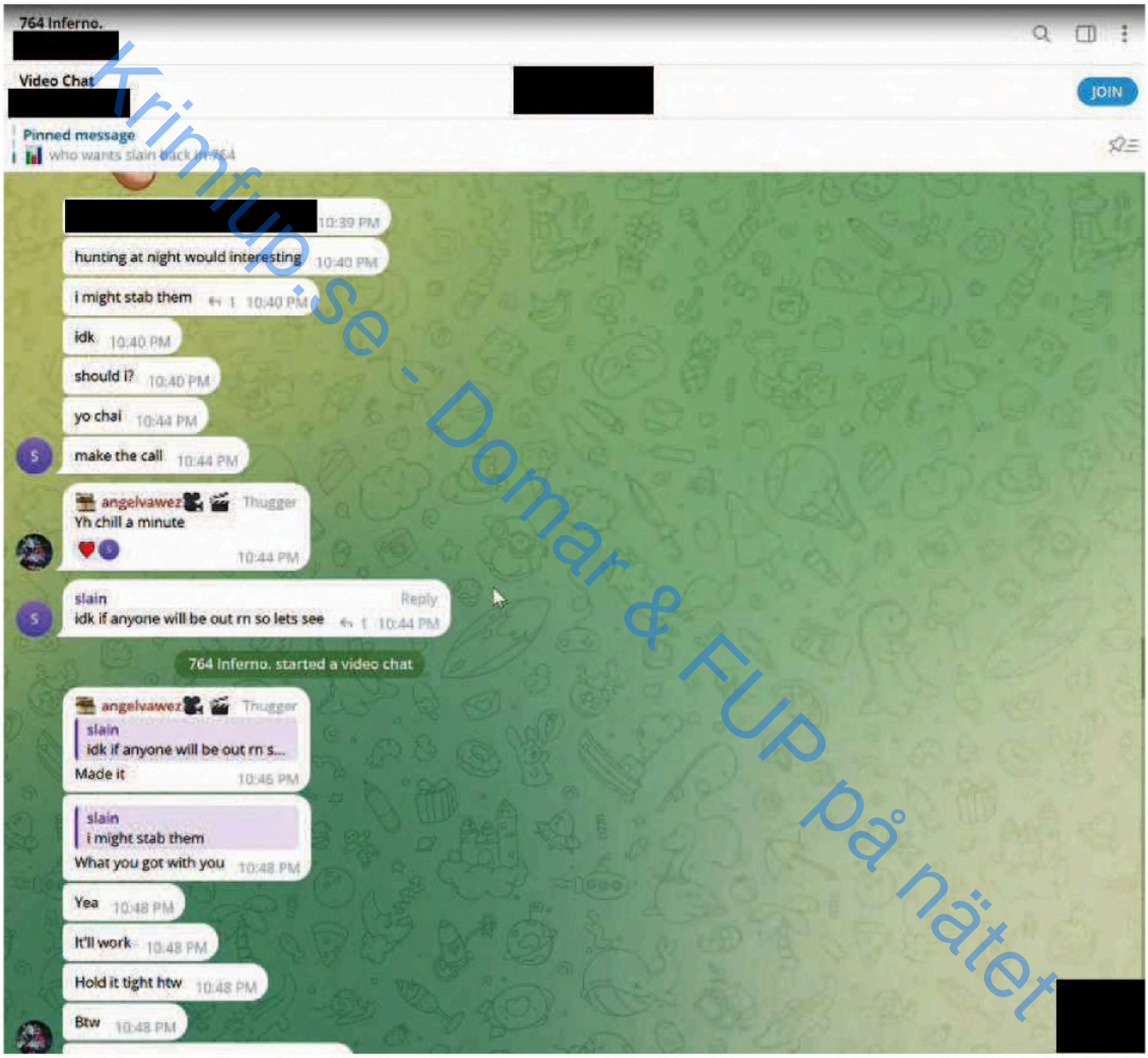
Originalhandlingens förvaringsplats	Datum	Tid
	2026-05-15	13:32

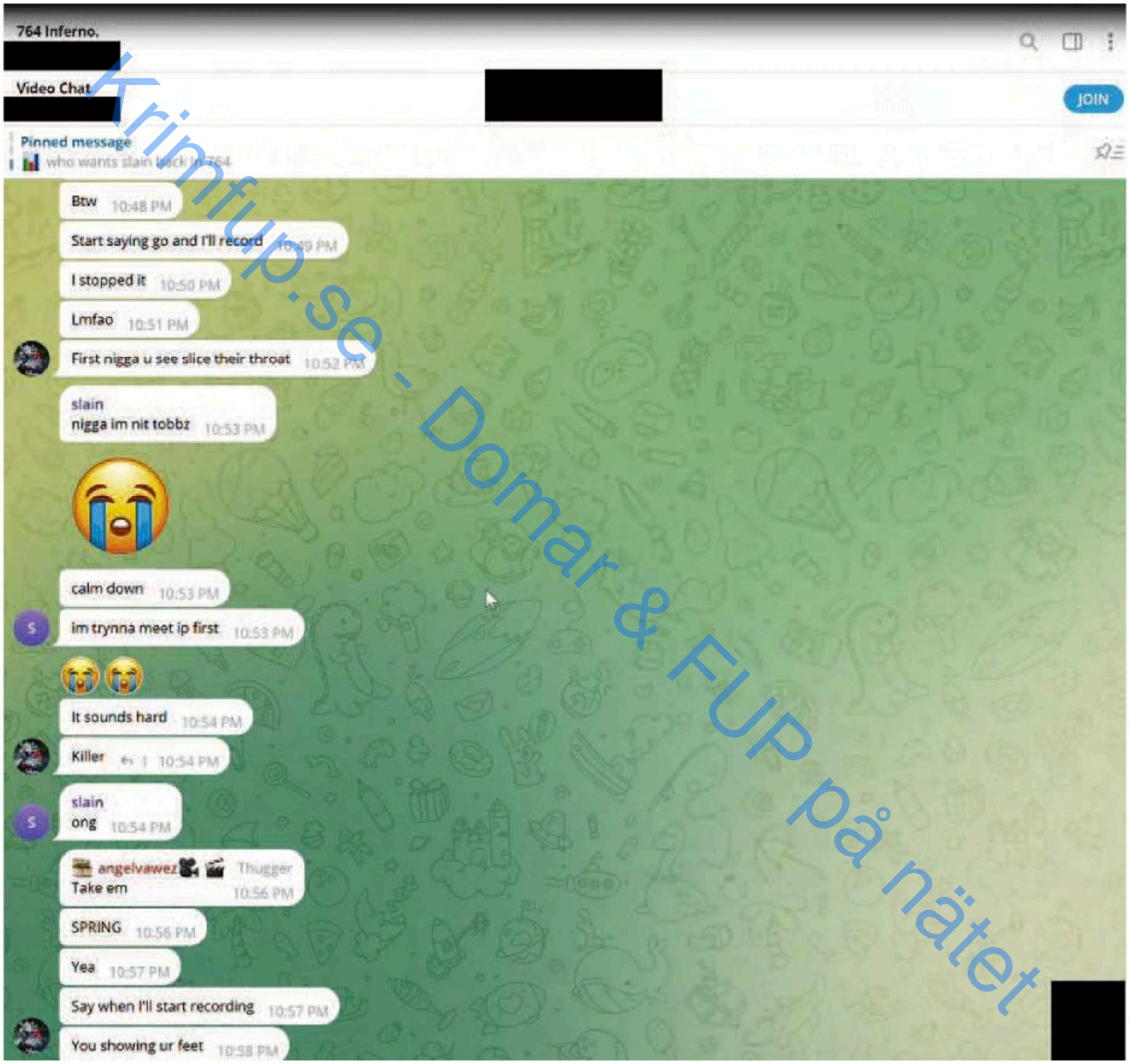
Involverad personal	Funktion
FE7B-B8VU	Uppgiftslämnare

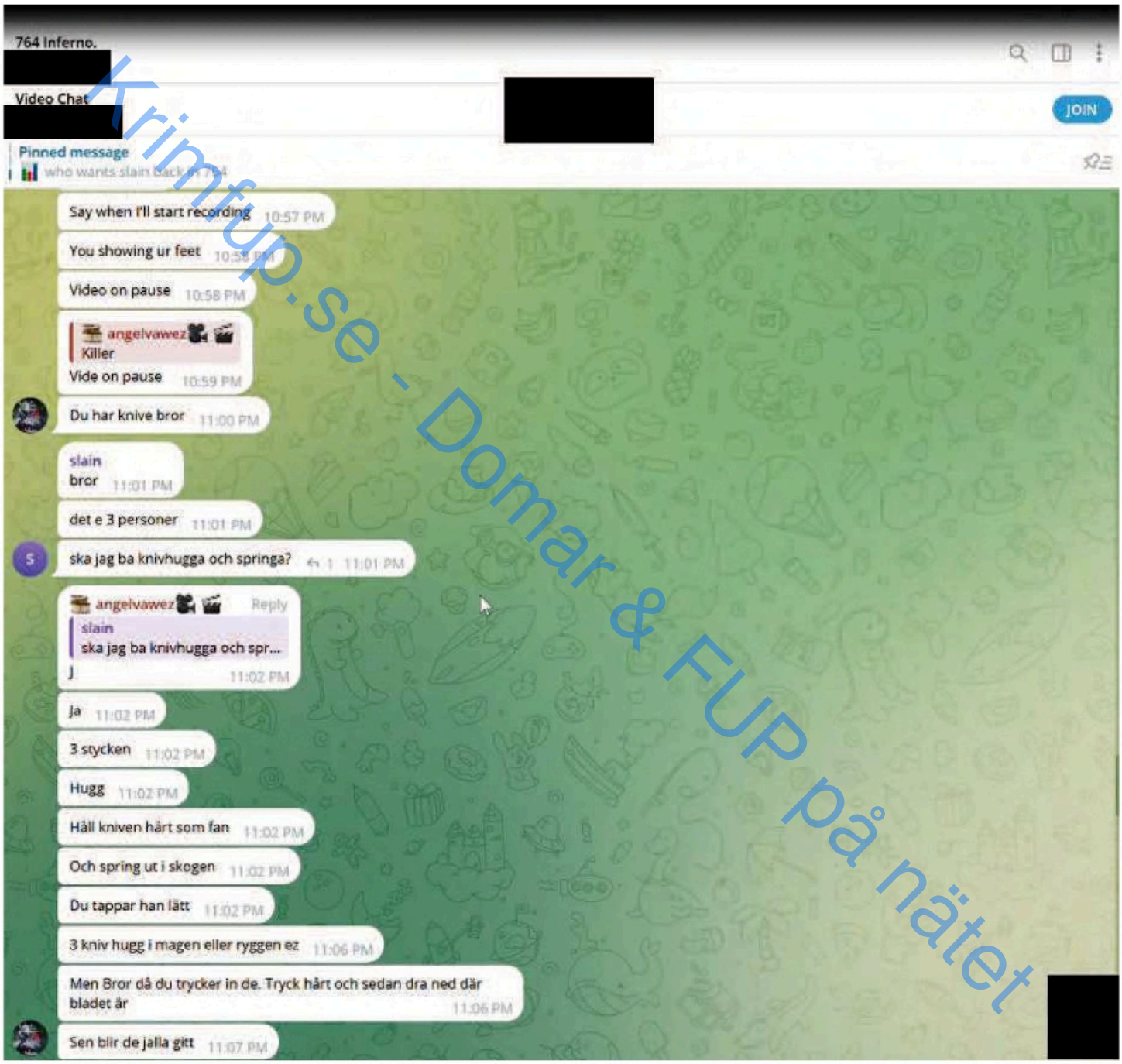
Berättelse

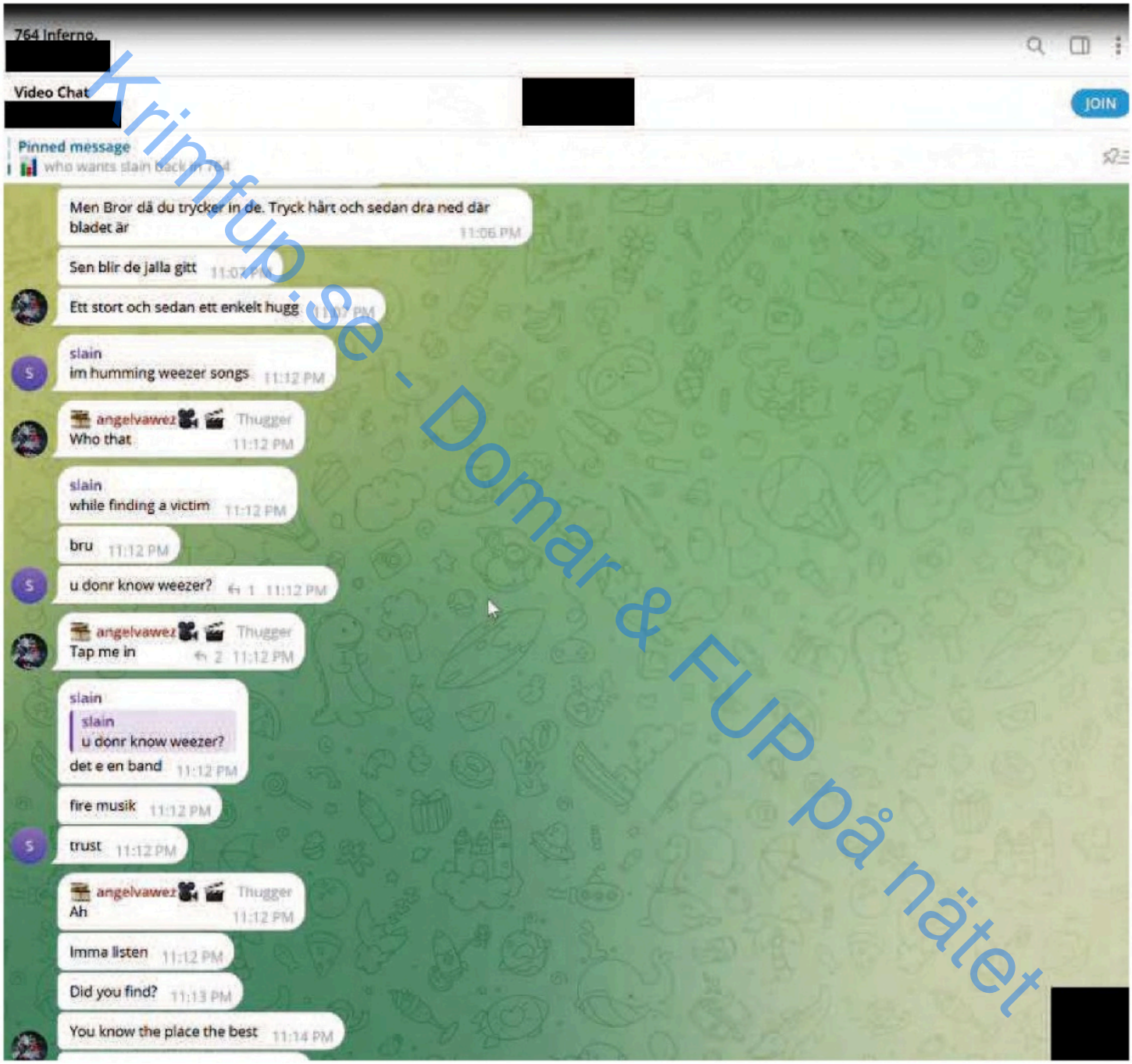
Från FBI (Bättre kvalitet)

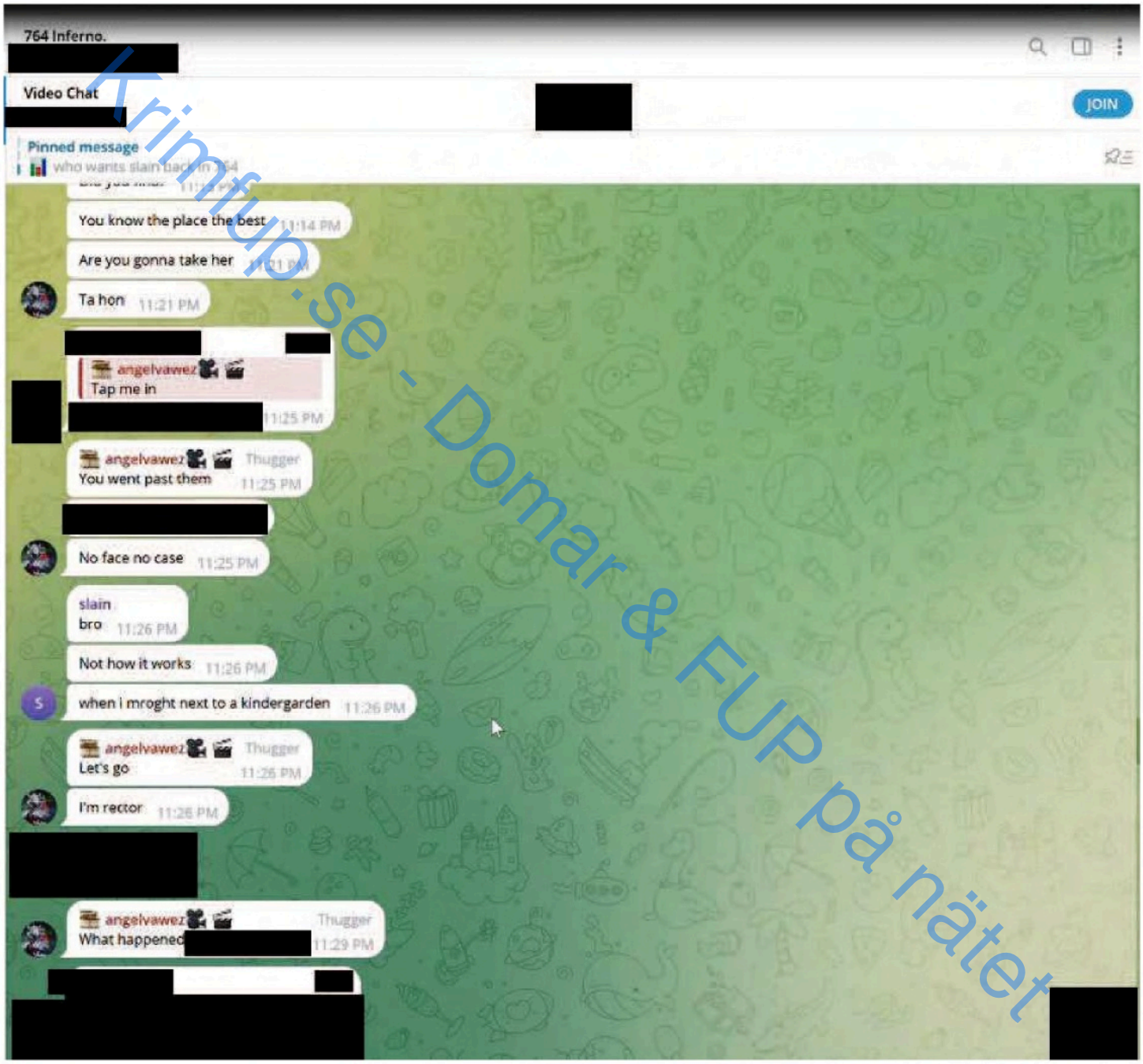


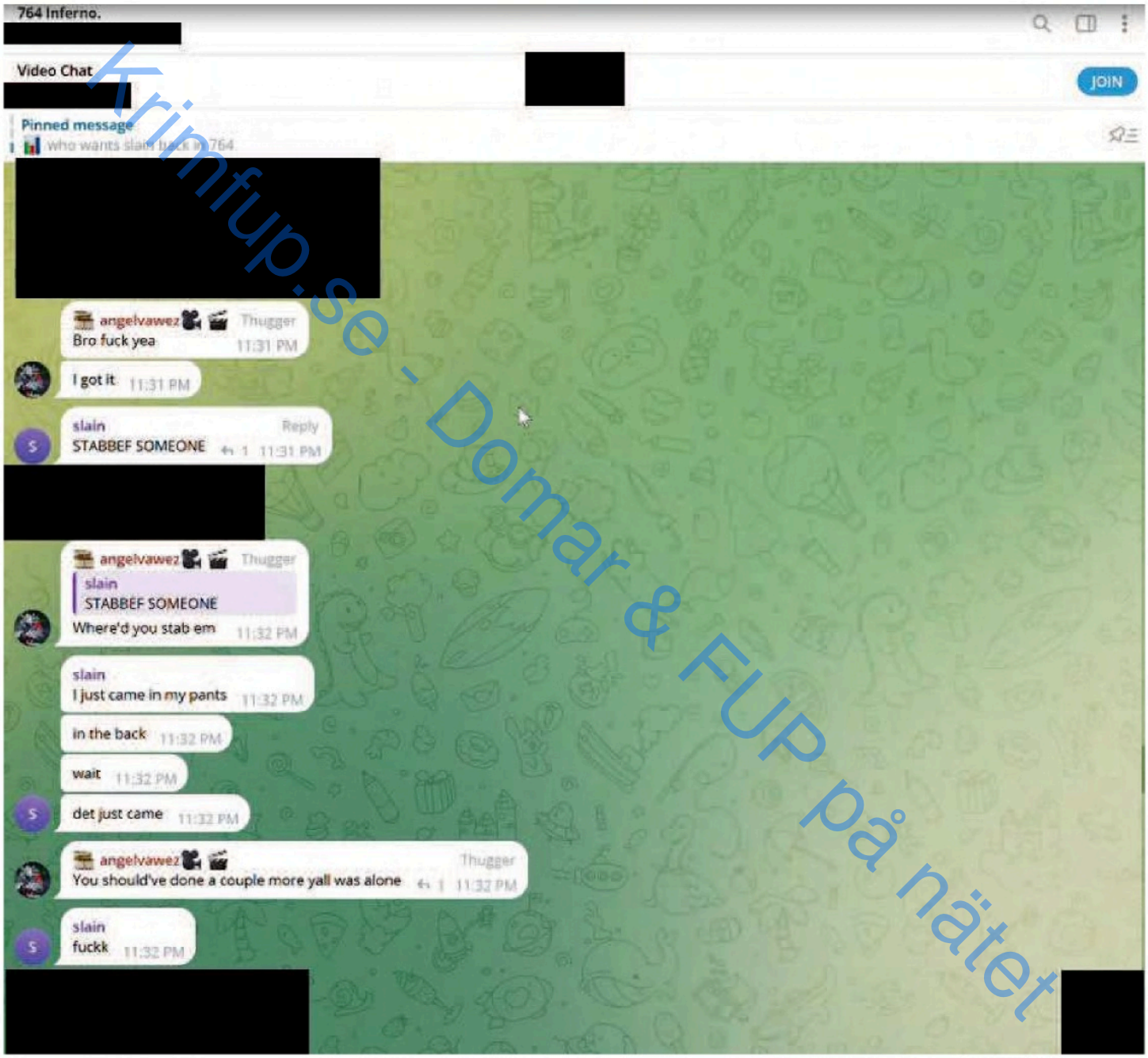


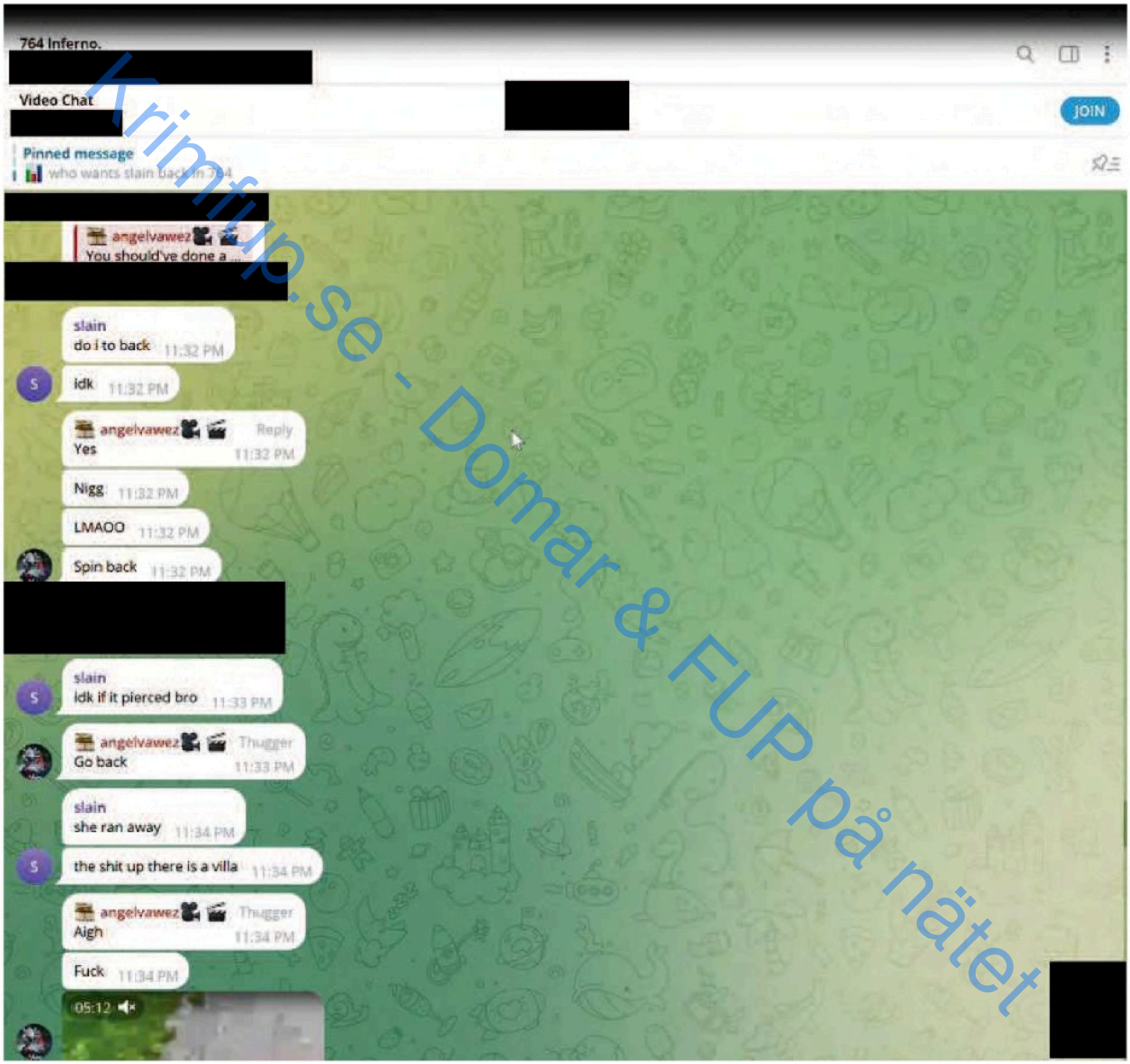


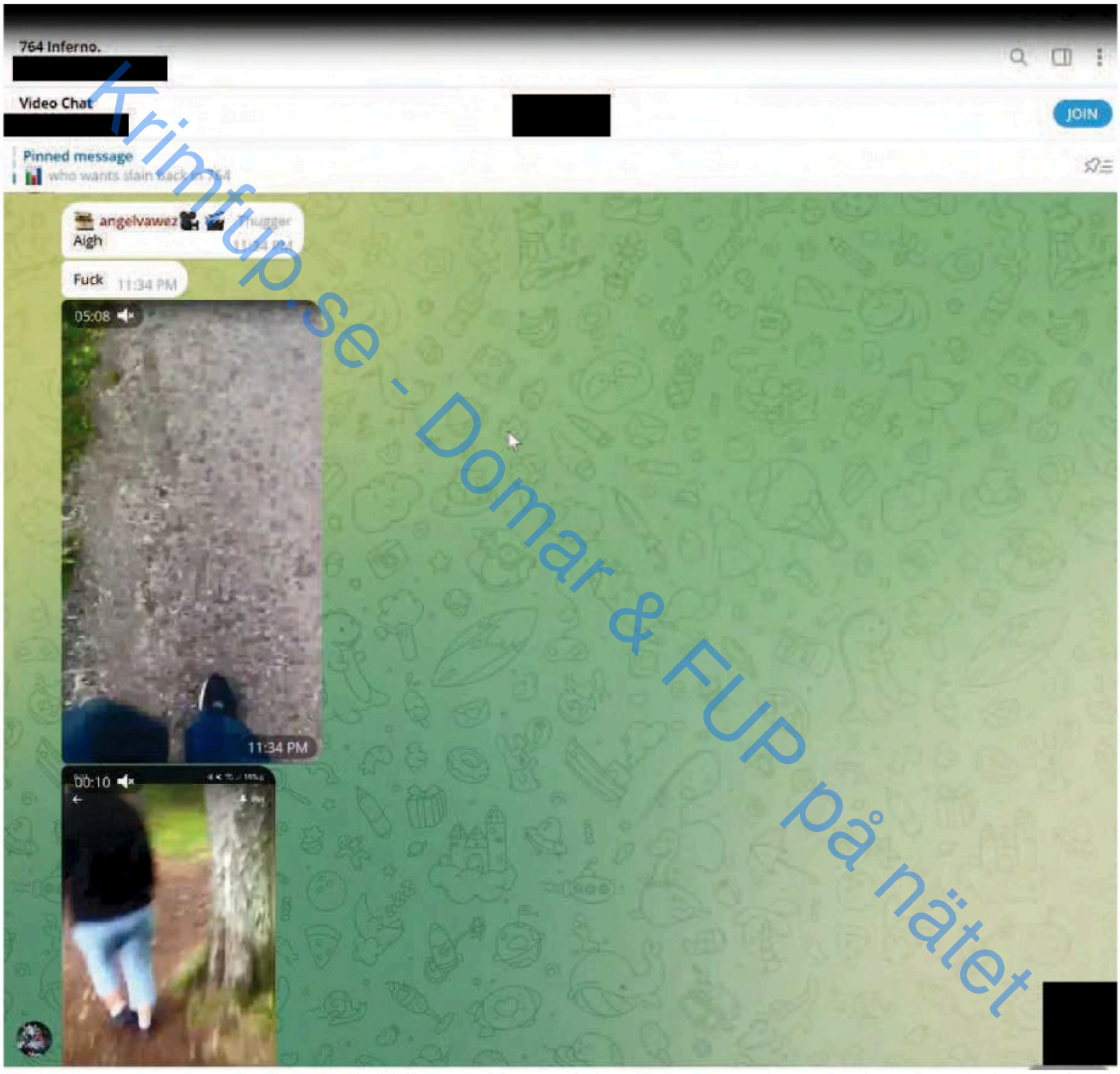


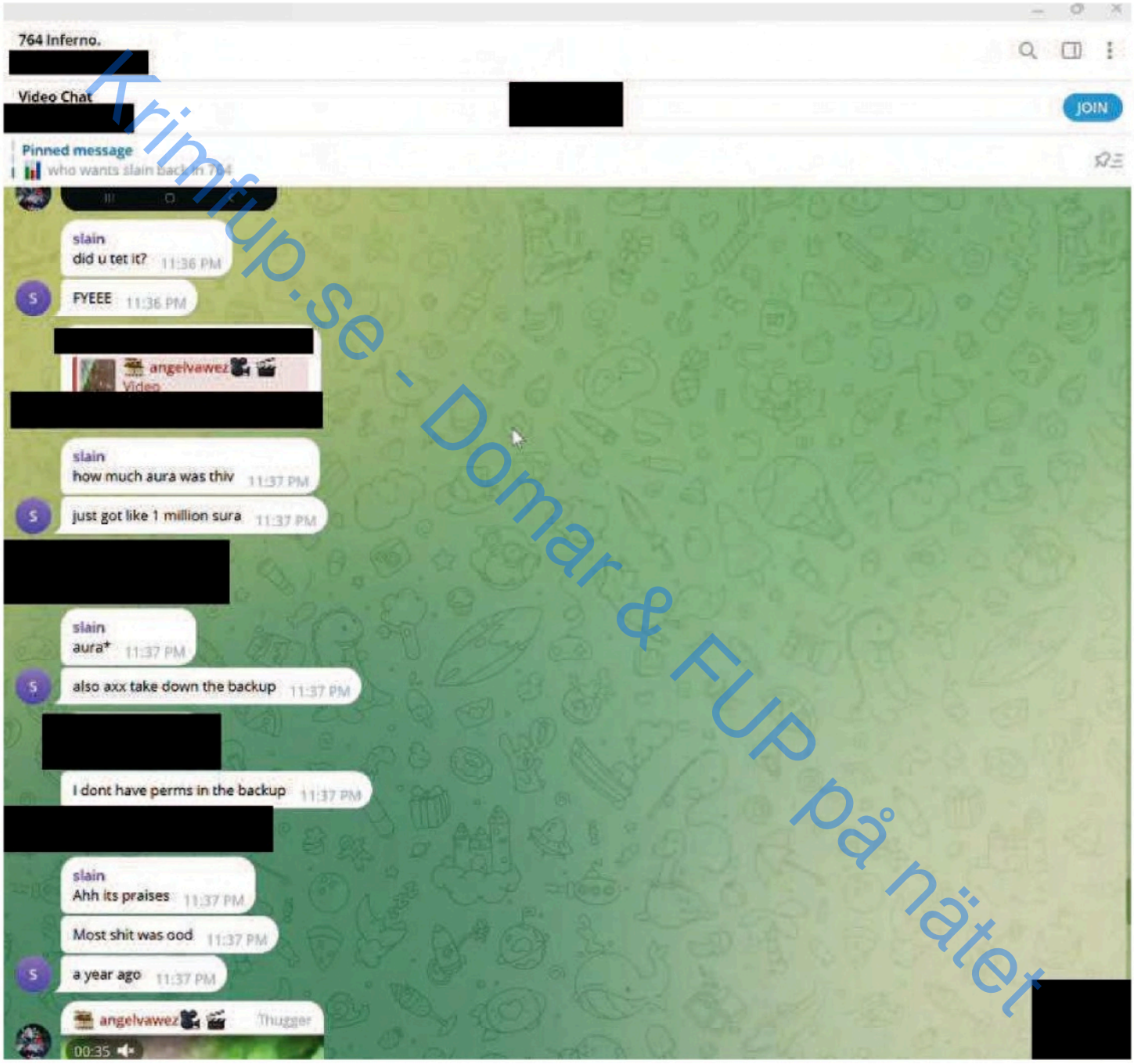


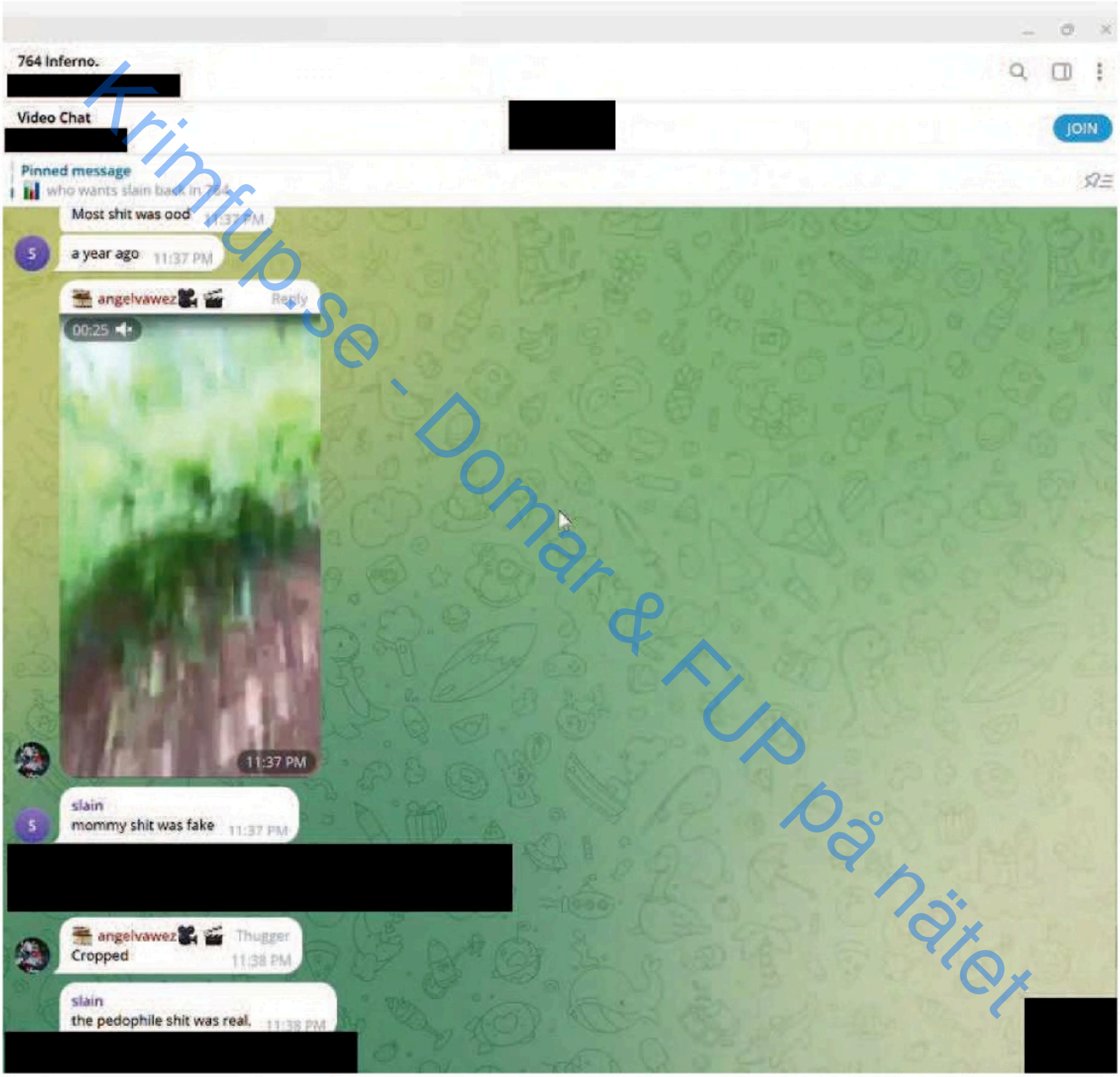


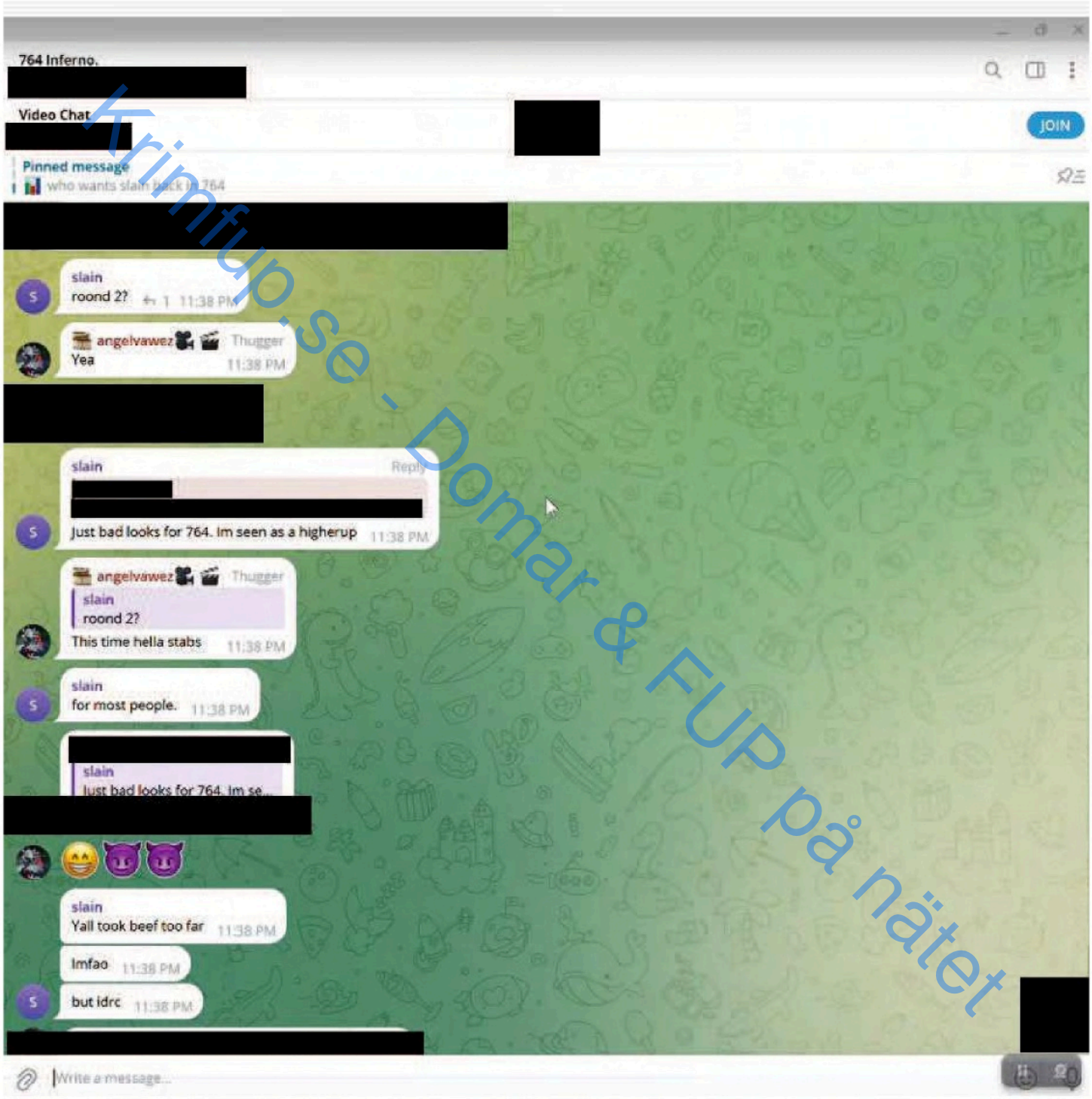


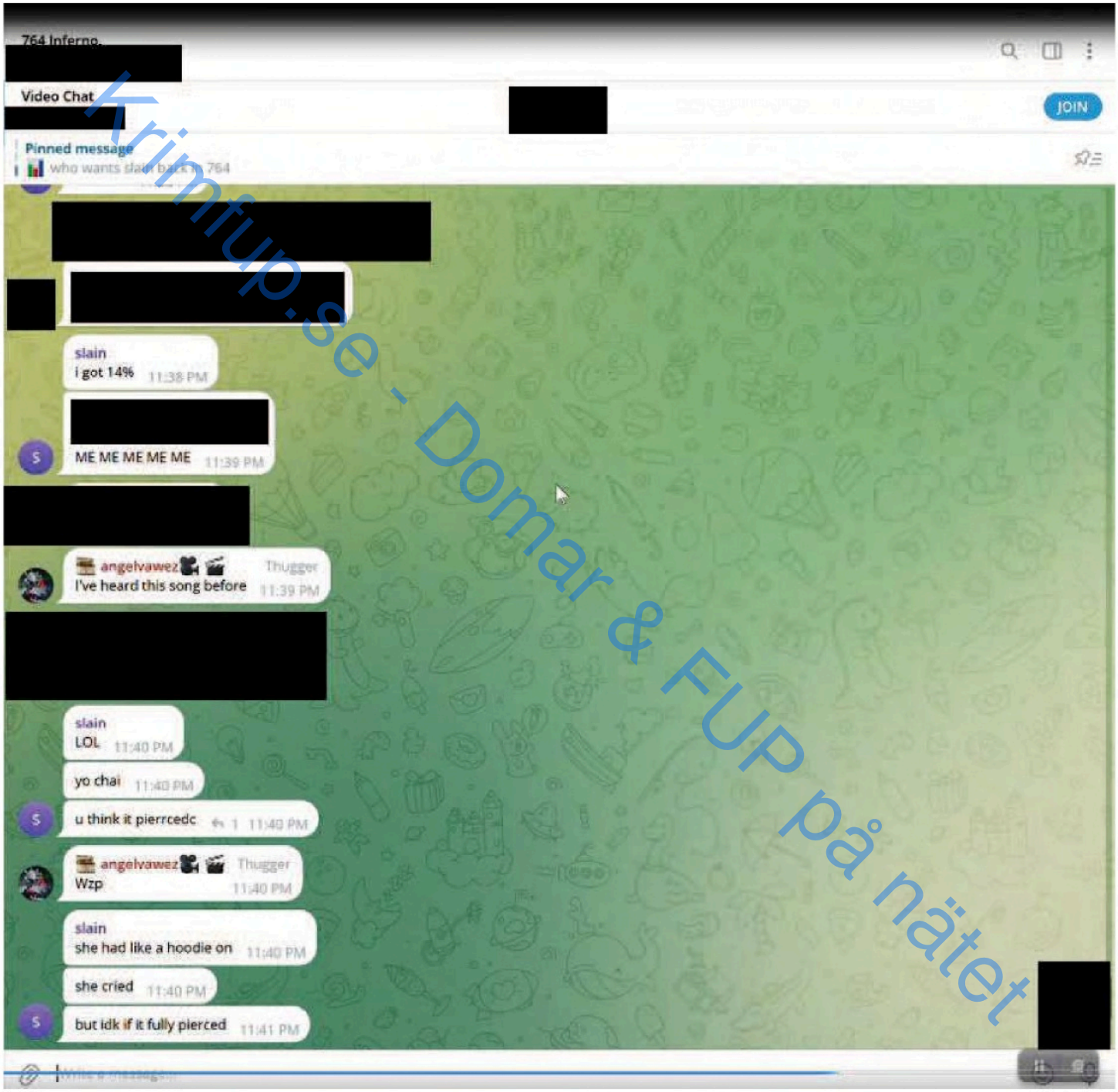


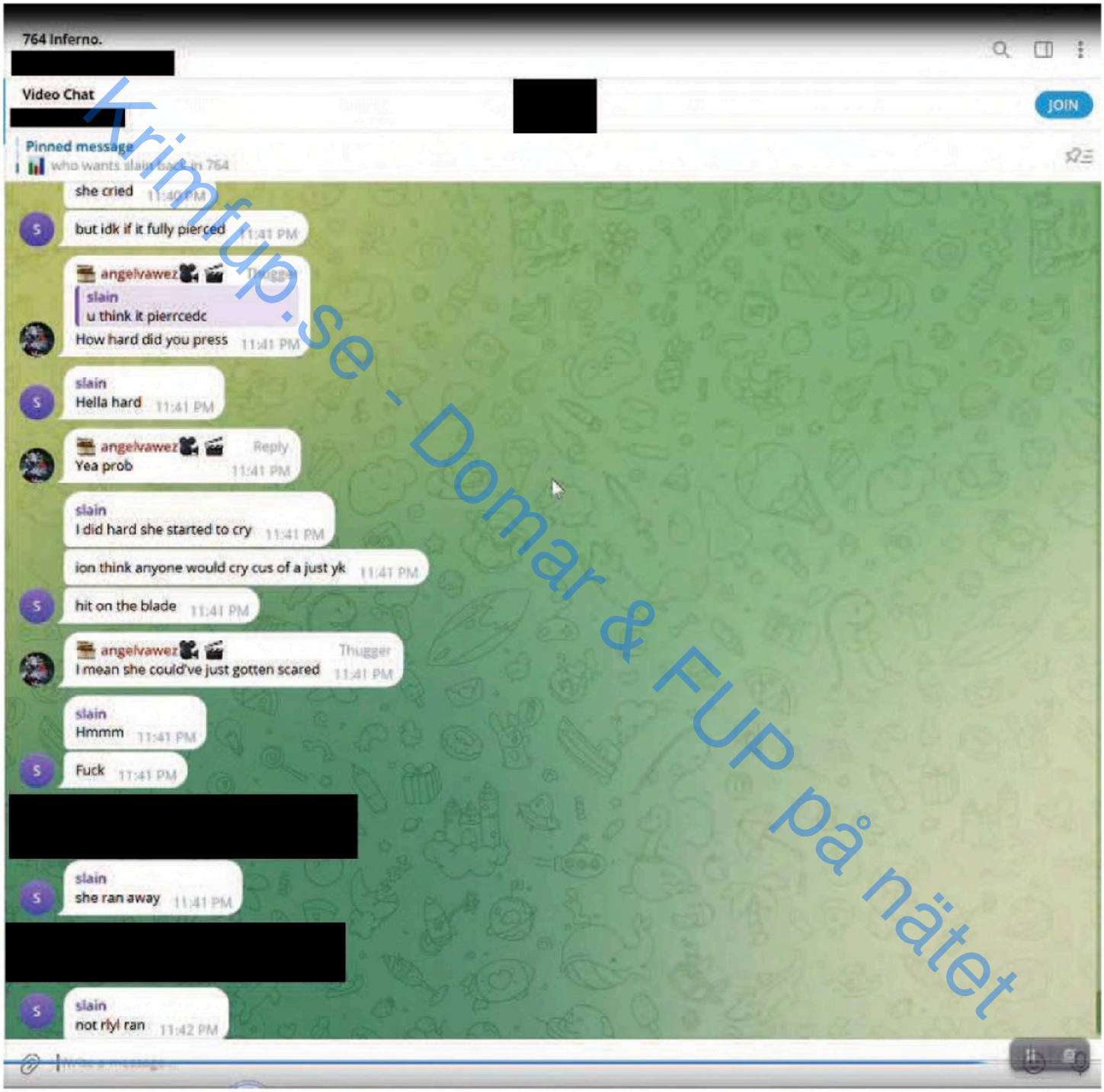












Polisen

Bilaga - Skäligen misstänkt

Enhet	Diarienr
Polisregion Nord, Utredning 3 LPO Umeå	5000-K287846-25

Skäligen misstänkt person	Personnr
Johansson, Peter Kevin Leonard	20070921-2450

Identifierad	Kontrollsätt	Kommentar
Ja	Känd av polisanställd	

Polisen

Personalia och dagsbotsuppgift

Utskriftsdatum
2026-05-15

Namn			Personnummer
Johansson, Peter Kevin Leonard			20070921-2450

Tilltalsnamn	Kallas för	Öknamn	Kön
Kevin			Man

Födelseförsamling	Födelselän	Födelseort utland
Holmsund	Västerbottens län	

Medborgarskap	Hemvistland	Telefonnr
Sverige		0722088133: Mobiltelefon

Postadress
Granfors 3
915 92 Robertsfors

Folkbokföringsort
Robertsfors

Föräldrars/Vårdnadshavares namn och adress (beträffande den som inte fyllt 20 år)

Utbildning

Yrke / Titel

Arbetsgivare | Telefonnr

Anställning (nuvarande och tidigare)

Arbetsförhet och hälsotillstånd

Kompletterande uppgifter

Muntliga uppgifter från misstänkt

Årsinkomst	Varav bidrag	Förmögenhet	Skulder

Hemmavarande barn under 18 år | Försörjningsplikt för barn under 21 år utöver hemmavarande barn

Inkomstkontroll

Fastställd förvärvsinkomst	För inkomstår

Kontrolldatum
- -

Övrigt
Övriga anteckningar

Polisen

Underrättelse/Delgivning jml RB 23:18a

Enhet
Polisregion Nord, Utredning 3 LPO Umeå

Ärende

Diarienr
5000-K287846-25

Underrättad av
FE7B-B8VU

Gärning
Övergripande

Berörd person

Personnr
20070921-2450

Efternamn
Johansson

Förnamn
Peter Kevin Leonard

Underrättelsesätt
Muntlig underrättelse

Datum för muntlig underrättelse
2026-05-15

Yttrande senast (rådrum)
2026-05-15

Notering
Mailat till försvarare samt lämnats till misstänkt på häktet

Misstänkt har getts möjlighet att ta del av materialet från den slutförda utredningen (RB 23:18a § / FUK 12 §)

Resultat av slutunderrättelse
Ingen erinran

Information gällande erinran

Försvarare

Namn
Töyrä, Emily

Underrättelsesätt
Muntlig underrättelse

Datum för muntlig underrättelse
2026-05-15

Yttrande senast (rådrum)
2026-05-15

Notering
Mailats till försvarare samt lämnats till misstänkt på häktet

Resultat av slutunderrättelse
Ingen erinran

Information gällande erinran