

NYHETSBREV

NR.14 / OKT 2026

INNEHÅLL

1. **Inledning** — Nicolas Fock
2. **Krönika** — Stefan Axelsson
3. **Forskningsnytt** — Johannes Olegård
4. **Forskningsnytt** — Johnny Bengtsson
5. **Du är kassakon i en cynisk förlagsvärld**
— Johnny Bengtsson
6. **Partner Spotlight** **När utredningens AI-assistent låter övertygande men har fel** — Jacob Isaksen,
Director of Advanced Solutions, DataExpert
7. **Globala AI-nyheter**
8. **Physical AI-robotik & Summer School 2027**
9. **Samlad länklista**

NÄSTA NÄTVERKSTRÄFF

Den 1:a december, 2026



Digital Forensics Sweden

is the formation of a cross-organizational network — a competence center with a national reach — operating in a global context.





1. INLEDNING

Kära läsare!

Att arbeta med digitala bevis idag handlar i allt högre grad om skala och precision. I takt med att mängden krypterad och ostrukturerad data ökar exponentiellt har AI gått från att vara en lovande teknologi till en nödvändig hörnsten i det forensiska hantverket. Automatiserad bild- och textanalys, anomalidetektion och säkrare bevishantering är bara några av de områden där utvecklingen just nu skapar stort värde i vardagligt arbete.

Inom Digital Forensics Sweden vill vi tillsammans med er driva på initiativ och skapa konkreta projekt för att på olika sätt stärka vårt ekosystem, och utforska nya teknikområden och tillämpningar av ny forskning och teknik. För att lyckas krävs ert engagemang, och era inspel, era idéer och era synpunkter.

I detta nyhetsbrev fördjupar vi oss i både tilliten till generativ AI, exempelvis kvalitet hos LLM:er, och får en introduktion till nyskrivna artiklar om metoder för att spåra 3D-printade vapen.

Vi introducerar också en ny sektion i nyhetsbrevet som vi hoppas ni kommer att uppskatta: Ett avsnitt där ni som partners kan bidra med erfarenheter, tankar eller berätta om det ni gör i er verksamhet eller med era produkter och tjänster.

Först ut är Data Expert och Jacob Isaksen som berättar om hur man använder agentisk AI för att skapa större kundvärde.

Kanske är det din organisation som skriver härnäst – hör av er så finns nu alla möjligheter till detta? Ge oss också gärna feedback på hur ni vill att vi ska forma nyhetsbrevet till en bra läsoplevelse.

Med förhoppning om trevlig och informativ läsning!
Niclas Fock

2. Krönika

Stefan Axelsson

Vad tittade du på igår? Om trafikanalys som går genom krypteringen

Vi har haft årets Cybersweden-konferens från Cybercampus som ordnades av oss vid Stockholms Universitet. Där presenterades mycket som har med LLM:er att göra, men även uppföljning till intressanta resultat från Chalmers som kanske inte har fått den spridning de förtjänar, så jag tycker det är intressant att sammanfatta dem. (Men det finns en koppling till LLM:er, läs till slutet för den.)

Så, jag får med jämna mellanrum frågan, oftast av studenter men ibland av journalister, om inte forensiken snart är körd nu när allt är krypterat. Svaret är som vanligt att det beror på vad man menar med "allt", och att krypteringen skyddar innehållet men sällan omständigheterna. Trafikanalys är ju ett hederligt gammalt hantverk som var gammalt redan när jag var ung, och den som vill ha ett aktuellt exempel på hur långt man kommer med enbart storleken och tidpunkten på paket behöver inte leta länge.

Ett riktigt bra sådant presenterades på USENIX Security i Seattle i augusti förra året, och dessutom av landsmän: Martin Björklund och Romaric Duvignau vid Chalmers och Göteborgs universitet. Artikeln heter "Endangered Privacy: Large-Scale Monitoring of Video Streaming Services" och handlar om att peka ut exakt vilken video någon tittar på, trots att hela strömmen är TLS-skyddad.

Själva läckan är ingen nyhet, den har varit känd sedan 2016 och den mest kända artikeln i genren är "Beauty and the Burst" från USENIX Security 2017. Mekanismen följer direkt ur hur modern strömmande video fungerar. DASH (och HLS) delar upp videon i segment på några sekunder, och varje segment kodas med variabel bitrate. En actionscen får fler bitar än en scen där någon sitter still i en soffa, och segmenten varierar därför i storlek på ett sätt som beror på innehållet. Eftersom de ligger som färdiga, statiska filer på ett CDN så är den variationen dessutom densamma varje gång, för alla tittare. Spelaren hämtar ett segment i taget, vilket ger den karaktäristiska skurvisa trafiken, och sekvensen av skurstorlekar är i praktiken ett fingeravtryck av videon.

Det som gör artikeln intressant är inte mekanismen utan skalan, och framför allt hur billigt det blivit. Tidigare arbeten har i huvudsak tränat maskininlärning genom att titta på samma video hundratal gånger, vilket fungerar men inte går att skala till mer än något tusental videor. Björklund och Duvignau hämtar istället fingeravtrycken direkt. Deras verktyg, som de döpt till karl, startar aldrig någon uppspelning utan hämtar manifestet och läser sedan antingen indexsegmentet, där byte-intervallen för alla övriga segment står, eller, som i SVT:s fall, gör helt enkelt en HTTP HEAD mot varje segment-URL och läser av Content-Length. Manifest och mediafiler går att hämta oautentiserat från CDN:erna; det är bara metadatan man behöver logga in för.

Resultatet är ett dataset som täcker hela bibliotek för tre tjänster: Amazon Prime Video, Max och SVT Play. 242 364 videor och drygt tre miljoner fingeravtryck, insamlade på mindre än ett dygn från en enda maskin, och då med bromsen i för att inte bli IP-blockerad. Bara SVT Play står för nästan 27 000 videor.

igenkänningen sker med ett k-d-träd över glidande fönster av åtta på varandra följande skillnader i segmentstorlek, plus en tidsseriemetod ovanpå som poängsätter kandidater över tid. Trädet kräver 152 GB minne, knappast orimligt för den som vill göra det här på allvar. Och det fungerar. Med en angripare som ser trafiken på nätverksnivå identifieras 898 av 900 strömmar, utan en enda felaktig identifiering. Bakom VPN, alltså med all trafik i en krypterad tunnel tillsammans med maskinens bakgrundsbrus, blir det 835 av 840. Även en passiv angripare som bara står utanför och lyssnar på 802.11-trafiken klarar sig bra, åtminstone så länge nätverkskortet hinner med. Nio skurar räcker för ett första svar, systemet behöver inte se början av videon, och det följer med när offret byter film.

Här kommer vi till det jag tycker är det verkligt hedervärda med artikeln, nämligen att författarna tar basfrekvensproblemet på allvar. Det är ju, som jag gnällt om sedan nittioalet, det som brukar fälla den här sortens detektorer: i verkligheten är nästan all trafik man ser något helt annat än det man letar efter, och då dränks de sanna larmen av de falska. Så istället för att nöja sig med sina egna videor matar de in 490 timmar "okänd" trafik, YouTube, Netflix, SSH, SCP och allt möjligt annat, och ser efter hur höga poäng systemet delar ut då. Högsta poäng någonsin blev 1,99 mot ett tröskelvärde på 2,2. Noll falsklarm, och en uppskattning på ungefär ett per månad och övervakad källa. Det är, milt uttryckt, ovanligt städat.

Vad betyder då detta för oss? Dels det uppenbara: den som har en pcap från rätt punkt i nätverket kan i efterhand säga vad någon tittade på, när, och var i filmen personen befann sig, utan vare sig nycklar, samarbete från tjänsten eller tillgång till klienten. Dels det mindre uppenbara, nämligen att detta är en indiciekedja och inte en identifiering. Fingeravtrycken åldras när tjänsterna kodar om material, och författarna noterar själva att ett par videor missades just av det skälet, samt att en del "felidentifieringar" visade sig vara speglar av samma film under ett annat video-ID. Den som tänker bära in ett sådant här resultat i en rättssal bör ha både insamlingsdatum och den sortens fallgropar klara för sig.

Motmedel finns, men de är dyra. Mullvads DAITA, som bygger på Maybenot-ramverket från Tobias Pulls i Karlstad (ännu en svensk i sammanhanget), stoppar angreppet men dubblar i bästa fall bandbreddsförbrukningen. Roten sitter i klienten: bufferten strävar efter att hålla en konstant nivå och avslöjar sig därför. Författarna föreslår slumpad buffert, flera segment per begäran och HTTP/2 eller senare. De påpekar klokt nog att enbart lika stora segment inte hjälper; då flyttar angreppet bara över till tidsdomänen.

Att detta i princip varit möjligt länge är ingen tröst. Jan Freese konstaterade redan på sjuttioalet att datorer tar bort manuella spärrar, alltså gör praktiskt genomförbart det som tidigare bara var teoretiskt möjligt, och det är precis vad som hänt här. Skillnaden mot 2017 är inte att läckan upptäckts, utan att den som vill övervaka en hel nationell public service-tjänst numera kan sätta upp det på en eftermiddag med kod som ligger öppet på GitHub. Författarna publicerar nämligen allt: verktygen, fingeravtrycksdatabasen, pcap-filerna och ett skript som reproducerar resultaten. Det ska de ha en eloge för; det är fortfarande sorgligt sällsynt och precis vad vi behöver för att kunna forska vidare på både angrepp och försvar.

****P.S.****

Jag noterar i förbifarten att SVT Play hamnade i studien delvis för att biblioteket är lagom stort och fullständigt kartläggbart. Public service har ju sina sidor.

För de av er som orkat så långt, vad är då kopplingen till LLM:er? Jo, det här är den första gången jag fuskat helt och hållet. Jag ville se hur bra LLM:er faktiskt blivit på att skriva artiklar, särskilt hur bra de blivit på att inte skriva som LLM:er. Så hela ovanstående är resultatet av att jag matade allt jag tidigare skrivit för nyhetsbrevet och bad Claude (Opus 5 Extra, så inte ens den mest avancerade modellen) att skriva om de här resultaten på samma sätt som om jag skulle gjort det.

Och f-n trot om den inte skriver som jag åtminstone lika bra som om jag själv skulle gjort det. Var det någon som hittade något som tydde på något annat. Och är jag ens författare till det här? "May you live in interesting times" indeed...

****Källor****

Endangered Privacy: Large-Scale Monitoring of Video Streaming Services, Martin Björklund och Romaric Duvignau, 34th USENIX Security Symposium, Seattle, augusti 2025, s. 6581–6597. Fritt tillgänglig:

<https://www.usenix.org/conference/usenixsecurity25/presentation/bjorklund>

Verktyg, dataset och capture-filer: <https://zenodo.org/records/14676527> samt

<https://github.com/trustcom/endangered-privacy>.

Föregångaren, med SVT Play och 20 000 videor: I see what you're watching on your streaming service: Fast identification of DASH encrypted network traces, Björklund m.fl., IEEE CCNC 2023.

Klassikern i genren: Beauty and the Burst: Remote Identification of Encrypted Video Streams, Roei Schuster, Vitaly Shmatikov och Eran Tromer, 26th USENIX Security Symposium, 2017.

Mullvad om DAITA: <https://mullvad.net/en/blog/introducing-defense-against-ai-guided-traffic-analysis-daita>

3. Forskningsnytt

Johannes Olegård

Vad är kvalitet?

Jag har tidigare forskat⁽¹⁾ på vad man ska stoppa i cybersäkerhetsrelevanta loggar för att de ska vara forensiskt nyttiga i efterhand. Framförallt handlar det om att inte missa viktig information, samtidigt som man inte vill drunkna i oviktig information—där kruxet alltså är att veta vad som är viktigt och ej, innan det hunnit bli viktigt. Nyligen har jag insett att även forensiska rapporter (alltså skrivna av människor) faktiskt har samma problem.

Det här problemet är en av flera "felkällor" i dokument, och även loggar och rapporter har sina egna typiska felkällor (t.ex. förfalskning respektive slarvfel)—så menar jag att det finns en underliggande "systematik" här som kan gå snett. När man skriver en rapport så följer man ju ett underförstått "recept" på hur en rapport ska se ut, precis som en logfil skrivs utifrån kod (ett extremt konkret recept). Det kan handla att man bara skriver rapporten ungefär på samma sätt från gång till gång (det finns ett mönster) eller att man faktiskt följer en checklista.

Mänskliga fel påverkar såklart exekveringen av sådana recept (för att det är monotont och tråkigt⁽²⁾), men jag menar att ett bra recept har en systematik som gör att man kan upptäcka felen i efterhand. Till exempel påverkar mänskligt fel även själva designen på receptet (framförallt i checklistor), vilket i sin tur påverkar hur receptet tolkas. Som del av den tolkning gör man också beslut av vilken "extra" information man behöver lägga till som inte tydligt specificeras i receptet. Till exempel, när jag försöker vara pedagogisk så nämner jag ofta ut (utvalda) extra detaljer, som inte är strikt nödvändiga, men som hjälper den andra personen upptäcka sina egna missförstånd—och det är den typen av tänk man vill ha när det gäller både loggar och rapporter.

Och då kan man ju tänka sig att, likt självkörande bilar, borde en LLM borde kunna lösa det här problemet genom att helt enkelt göra färre misstag än människor. den tröttnar inte, den håller koll på senaste tekniken, och har expertis från andra områden. Men, när vi pratar om varför vi inte bara låter LLMer skriva rapporter åt oss, så handlar det just om att introducera fel (hallucinationer, etc.).⁽³⁾

Det kommer dock bättre och bättre LLMer med tiden. Hade vi då kunnat nå en punkt där LLMens egna fel är så få att de klår människor i att skriva rapporter? Nja, inom just forensiken finns det anledningar bortom felkällor att inte använda LLMer. Framförallt rör det sig om icke-determinism⁽³⁾ (det ska inte bli olika resultat varje gång man skriver rapporten, eller när någon annan försöker återskapa resultaten), principen att man inte vill bli åtalade och dömd helt av robotar, och—framförallt—att robotar inte kan åta sig "ansvar" (liability, ansvar med konsekvenser). Om en människa gör ett misstag, så bestraffas ofta denne—den "har ett ansvar". Så, på sätt och vis, bygger vårt nuvarande system på att hota människor med våld om de inte presterar—och det funkar inte att hota en LLM med våld.

Det lustiga är att LLM-fel är skrämmande likna mänskliga fel. Formuleringen av en fråga påverkar svaret. Varje gång vi minns, så skrivs minnet om—och stämmer alltså inte helt med verkligheten (likt LLM-hallucinationer). Vår uppväxt (training) ger oss fördomar, och påverkar vår kapacitet att ens uppfatta världen (om man tror världen består av två kön, så blir snabbt alla indikationer på motsatsen osynliga). Så varför låter vi ens människor nära rättsprocessen!? Hot löser inte de här problemen!

Så lösningen ligger kanske inte i att minska hur mycket fel LLMer gör (för fel kommer alltid finnas oavsett vem eller vad som gör jobbet), utan vår möjligheter att rätta till fel i efterhand—vilket vårt rättssystem ju inte alltid har helt lätt med. Kanske är inte problemet att LLMer "kan göra fel", utan att de pekar ut problem i systemet som alltid fanns där?

Inom IT-forensik, har vi länge haft ett problem med felfrekvenser (error rates)(4), och den kanske förvånande anledning till det är att en IT-forensika artefakt har en stor "mänsklig" komponent—man brukar säga att vi är mer som arkeologer än forensiker. DNA är DNA (mer eller mindre), men är ett stycke platt metall alltid en kniv? Vi kan testa ett verktyg korrekt kodar av en artefakt, men vi kan inte återskapa de omständigheter som skapade artefakten—för de är mänskliga omständigheter. Försöker vi skära ner situation till något konkret (t.ex. experiment i Windows-miljö), så har vi också skurit bort den mänskliga komponenten som gjorde artefakten intressant till att börja med. Det visar sig att ganska många områden inom forensiken har problem med felfrekvens(4).

LLMer har låtit oss börja automatisera "tolkning" (Interpretation i IT-forensiska processen), men vi har faktiskt aldrig varit särskilt bra på att verifiera forensiska resultat även innan LLMer. Det bästa vi har är att en annan person upprepa en undersökning och ser om de får samma resultat (liknande rapport)—men även om de får det, så är inte det nödvändigtvis rätt resultat. Det gäller att inte blanda ihop "tillförlitlighet" (reliability) med kvalitet—att ett program krashar konsistent (samma resultat varje gång!) betyder inte att det är ett bra program. På grund av detta har IT-forensisk forskning länge fokuserat på processen (göra rätt) snarare än resultaten (bli rätt).

Förmodligen har insisterandet på "felfrekvenser" alltid orealistiskt. Statistik är fel verktyg får något så nischat som IT-forensik—vi kommer aldrig ha tillräckligt med data när vi behöver den (utan att gå 1984-vägen). Vi har försökt att verifiera kvalitativa resultat med kvantitativa metoder. Såklart det inte funkar.

(1) <https://doi.org/10.1016/j.fsidi.2025.301877>

(2) <https://doi.org/10.1016/j.fsidi.2022.301351>

(3) <https://doi.org/10.1016/j.fsidi.2023.301609>

(4) https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_forensic_science_report_final.pdf

4. Forskningsnytt

Johnny Bengtsson

Publicerad artikel om 3D-skrivare

På skrivfronten intet nytt. Dessvärre är progressen nära stillastående på skrivfronten. Åtminstone gällande kappan till sammanläggningsavhandlingen.

Men på jobbfronten händer det spännande saker i stort sett hela tiden. Det ger idéer till nya intressanta uppslag. Ett exempel är den tilltagande förekomsten av 3D-skrivare som har figurerat i samband med förekomst av exempelvis 3D-vapen och knogjärn.

I lagen (1988:254) om förbud beträffande knivar och andra farliga föremål, 2 § går det exempelvis att läsa följande: *Knogjärn, kaststjärnor eller andra sådana föremål som är särskilt ägnade att användas som vapen vid brott mot liv eller hälsa samt springstiletter eller springknivar får inte överlåtas till personer under 21 år eller saluhållas. Lag (1990:413).* Det är med andra ord aja-baja att även inneha 3D-utskrivna knogjärn. Annat var det före 1990, då det tillverkades hemmagjorda kaststjärnor och nunchakus: något som förmodligen var mer skadligt för utövarna själva än för omgivningen – och där bibeln för omyndiga pojkar stavades Hobbex. Tänk, så många fina luftpistoler och kastknivar som såldes då.

Idag börjar förekomsten av 3D-skrivare sakteliga smyga sig på även i kontexten hemmafabriker. Inte för att det ännu är ett stort problem, men en växande trend. Traditionellt sett, så är det additiva området relativt utforskat även inom akademien. Fokuset har, enligt min mening, främst varit betonat på traditionell forensik, som spårjämförelser, vapenundersökningar, kemiska analyser av filament, et cetera.

Jag tycker mig ha sett att det endast har funnit ett ringa it-forensiskt forskningsfokus. Det jag har funnit har mestadels varit särartsfrågor med tveksam förankring bland praktiker. Det är naturligtvis behjärtansvärt att jättestora forskningsresurser har lagts på att finna metoder som analyserar RAM-dumpar i syfte att finna spår av G-code-filer, alltså 3D-skrivarinstruktioner för att skriva ut ett specifikt objekt. Detta är kanske mindre hjälpsamt för oss får döda (= ej driftsatta) beslag inskickade för undersökning. Att generera G-code-filer är en sak, men att gå hela vägen och skicka över dem till en 3D-skrivare och skriva ut – det är minsann något helt annat! Men där kanske lagstiftningarna skiljer sig åt mellan länderna.

I samband med två likartade 3D-skrivarärenden har jag funderat över möjligheten att delvis täcka över ett it-forensiskt forskningshål, parallellt med att klura på en intern metodbeskrivning. Tillsammans med min kollega Thomas, så har vi slutligen lyckats ro djävulen i land. Nu kan även du läsa vår publicerade artikel [1]. Och jo, vi har numera en fastställt metodbeskrivning.

[1] Bengtsson, J. och Adolfsson, T. (2026). **Digital forensic artefacts in Linux-based Creality 3D printers operating on Klipper firmware: Real-world case studies.** *Forensic Science International: Digital Investigation*, vol. 59 (302200). DOI: [10.1016/j.fsidi.2026.302200](https://doi.org/10.1016/j.fsidi.2026.302200).

5. Du är kassakon i en cynisk förlagsvärld

del 1

Johnny Bengtsson

Jag har sedan ett tag tillbaka fått en ny våg med spam adresserad Prof. Bengtsson eller Dr. Bengtsson. Nu är jag varken eller. Budskapet i innehållet ser däremot ungefär likadant ut: ”Åh, vi såg din artikel om [någon av mina publikationer] och vill att du publicerar din nästkommande artikel den i vår tidskrift som är inom fältet [biologi/medicin/management/smarta elnät/kvalitativ forskning inom turism/andra eljest forskning].”, ”Vi råkar har lite plats kvar till vårt nästa nummer. Deadline är snart, så skynda på att skicka in!”, ”Vi vill att du blir en medlem/reviewer i vår editorial board”, ”Vi skrev ett brev till dig den [datum], men du svarade inte. /.../ [Inklistrat spam från tidigare sant eller påstått meddelande]” eller ”Vi uppskattar din artikel X och bjuder in dig som talare på vår konferens (med oklart syfte och målgrupp). Här är andra talare som redan är spikade (m.a.o. folk som antingen har blivit duperade, alternativt att arrangören har kapat deras namn, bild och affiliering)”.

Rovtidskrifter och rovkonferenser

Det är knappast en underdrift att påstå att spammejlerna ger ett AI-genererat intryck; affärsidéerna syftar främst på en sak: avancerat bondfångeri genom smicker och utfästelser. Fenomenet är välbekant: rovtidskrifter[1], även rovdjurstidskrifter, (eng. predatory journals) respektive rovkonferenser (rovdjurskonferenser, predatory conferences), verksamheter som utger sig för att vara seriösa men i praktiken bygger på en affärsmodell där både juniora och seniora forskare cyniskt låter sig utnyttjas.

Den affärsmässiga verksamheten kring denna typ av verksamhet kännetecknas av en till synes vetenskaplig integritet, en extremt generös acceptansgrad, dubiös eller helt utebliven oberoende vetenskaplig granskningsprocess (peer review) samt ett brett och ospecifikt fokus utformat för att locka så många potentiella forskare som möjligt. Därtill hör att de sällan eller aldrig indexerats i bibliometriska databaser som exempelvis Scopus[2], Web of Science [3] eller SCImago[4], även om motsatsen påstås. I praktiken innebär detta att du som författare skickar in ditt manus, det passerar ett skenbart editorial board, ”granskas” och slutligen accepteras, varefter du faktureras en publiceringsavgift i form av en APC (Article Processing Charge).

Det sistnämnda är i sig inte så konstigt, då även väletablerade förlag använder en liknande avgiftsmodell för att göra artiklar fritt tillgängliga, alltså open access. Skillnaden ligger i att seriösa förlag faktiskt tillhandahåller en transparent och rigorös granskningsprocess – något rovdjurstidskrifter saknar.

[1] Språktidningen (2019). <https://spraktidningen.se/sprakbloggen/veckans-nyord-rovdjurstidskrift-rovtidskrift/>

[2] Scopus. <https://www.scopus.com>

[3] Clarivate. Web of Science platform. <https://clarivate.com/academia-government/scientific-and-academic-research/research-discovery-and-referencing/web-of-science/>

[4] SCImago Journal & Country Rank. <https://www.scimagojr.com/>

Det akademiska ekosystemet

Varför tycks rovfenomenet ändå bära sig som affärsidé? Jag har under senare tid stött på begreppet publish or perish – ett slags destruktivt ekosystem som fortfarande tycks förekomma inom vissa osunda forskningskulturer, där det finns förväntningar på forskare ständigt ska vara relevanta genom ständigt nya publikationer och vara synliga i så kallade ”internationella” konferenser.

Att då ta en genväg via rovdjurstidskrifter kan därför locka vissa; din artikel ser ljuset i en ”internationell tidskrift” utan att du behöver krångla med en massa vetenskapliga ifrågasättanden. Du betalar endast en APC:n, så borde allt vara klart. Eller? Bortsett från att du inte får ditt manuskript vetenskapligt prövat, är den stora nackdelen att du riskerar att kasta alla dina nedlagda forskningsresurser i en bottenlös önskebrunn. Du kan inte meritera dig med en artikel som publicerats i en låstidskrift. Förmodligen kommer du också behöva förklara ett och annat vid ett eventuellt akademiskt avancemang. Men som sagt, det finns även seniora forskare som låtit sig förföras av smicker och löften om ett granskningssnabbspår.

En annan aspekt av publish or perish rör löpande intäkter: nya forskningsmedel, fortsatt forskning. I många fall ser jag problemet snarare som en inlåsningsseffekt. Forskaren kan välja att fortsätta den inslagna forskningsbanan; att frivilligt bryta ny mark inom ett annat fält där forskaren är akademiskt omeriterad, gissar jag innebär en risk: både i termer av uteblivna anslag och förlorad tid. Har man dessutom en eller flera doktorander eller postdoktorer att föda, så är en ny inriktning för med sig negativa konsekvenser. I slutändan ser jag att rovfenomenet främst syftar till att vara en forskningsetiskt tveksam möjliggörare för tidspressade forskare och doktorander som vill köpa sig fria från den akademiska undergången (perish) – men även lärosäten eller institutioner som råkar vara beroende av anslag som styrs av synlighet.

Erkända tidskrifter

De etablerade vetenskapliga tidskrifterna som regelmässigt publicerar forskningsresultat i form av artiklar och konferensbidrag är, å sin sida, löpande utsatta för bibliometriska utvärderingar. För att förenkla för oss som står utanför eller lite vid sidan om den akademiska världen, så rankas tidskrifterna i kvartiler, från Q1 till Q4. Denna indelning baseras på olika bibliometriska mått som exempelvis citeringsfrekvens och tidskriftens relativa genomslag inom sitt ämnesområde. Q1-tidskrifter tillhör den övre fjärdedelen (topp 25%) och anses ha högst vetenskaplig tyngd, medan Q4-tidskrifter ligger i den nedre fjärdedelen.

Det är samtidigt viktigt att förstå att kvartilrankningen är relativ och ämnesspecifik. En tidskrift kan därför rangordnas lägre eller högre beroende på vilken kategori den jämförs inom. En ren it-forensisk tidskrift kan exempelvis hamna lägre när den placeras i en bredare datavetenskaplig kategori med helt annan forskningsinriktning, medan samma tidskrift kan värderas betydligt högre bland tidskrifter som är nischade mot forensik – ännu högre i jämförelse med andra it-forensiska tidskrifter. Kvartilerna säger med andra ord något om tidskriftens genomslag inom den bedömda kategorin, inte om dess absoluta kvalitet i termer av metodik och forskningsresultat.

I sammanhanget är det viktigt att betona att en Q4-tidskrift i sig är lågkvalitativ eller ligger i paritet med rovtidskrifter; många mindre eller mer nischade forskningsfält har helt enkelt lägre citeringsvolym. Det kan exempelvis bero på att behovsägarna av forskningsresultatet inte nödvändigtvis själva bedriver forskning, som exempelvis it-forensiker. Detta tänkte jag närmare beröra i nästa del samt reflektera över varför det tycks råda ett gap mellan akademien och praktiker och dess följdverkan för den it-forensiska forskningen.

Johnny, en enkel tjänsteman

Källor

Om du vill fördjupa dig i ämnet så finner du några svenskspråkiga källor här:

Per-Olof Eliasson (2022). Rovtidskrifter är ett växande problem. Läst: 2026-09-21.

<https://universitetslararen.se/2022/05/02/rovdjurstidskrifter-ar-ett-vaxande-problem/>.

Svenska handelshögskolan, Hanken. Rovpublicering. Läst: 2026-09-21.

<https://www.hanken.fi/sv/forskning/publikationer/publicering/pa-hanken/rovpublicering>.

Kungl. Ingenjörsvetenskapsakademien (IVA) (2022). "PUBLISH OR PERISH", Hur upplever forskare som är aktiva i utåtriktade aktiviteter konsekvenserna av bibliometrisk styrning?

En studie inom IVAs projekt Agenda för forskning. <https://libris.kb.se/p718qgp13zl935g>.

Läst: 2026-09-21.

Sara Nilsson (2018). Rovdjurstidskrifterna vinner mark.

<https://www.tidningencurie.se/nyheter/rovdjurstidskrifterna-vinner-mark>. Läst: 2026-09-21.

Universitetsbiblioteket, Karolinska Institutet (2026). Oseriösa tidskrifter. Läst: 2026-09-21.

<https://kib.ki.se/publicera-analysera/strategisk-publicering/oseriosa-tidskrifter>.

Karin Persson (2024). Så kan forskare räddas undan rovtidskrifterna.

<https://www.biblioteksbladet.se/nyheter/oppen-vetenskap/sa-kan-forskare-raddas-undan-rovtidskrifterna/>. Läst: 2026-09-21.

Tapio Salmi (2015). Publish or perish.

<https://blogs.abo.fi/forskarbloggen/2015/05/10/publish-or-perish/>. Läst: 2026-09-21.



6. PARTNER SPOTLIGHT

— INIFRÅN BRANSCHEN

Jacob Isaksen
Director of Advanced Solutions
DataExpert

När utredningens AI-assistent låter övertygande men har fel

DataExpert hjälper polis, åklagare, skatte-, tull- och ekobrottsutredare samt företagens egna utredningsteam att få ut mer av de forensiska verktyg de redan köper av oss, t.ex. Nuix, Magnet, Cellebrite, MSAB, Exterro med flera. Vi har nyligen byggt en agentisk AI-assistent som arbetar tvärs över de verktygen. Utredaren ställer en fråga eller formulerar en hypotes med vanliga ord; assistenten söker i bevismaterialet, resonerar kring träffarna, söker igen i flera iterationer och lämnar ett svar. Den här texten handlar om varför ett sådant svar kan låta övertygande och ändå vara fel, och vad som krävs för att hindra att det händer.

Exempel: En utredare i ett bedrägeriärende frågar vem som tjänade på en penningöverföring. AI-assistentens svar är ett textstycke som ser relevant ut. Det knyter ihop en betalning, ett bolag, ett namn och en faktura. Det ser ut som ett riktigt fynd. Två frågor avgör om så är fallet: vad såg AI-assistenten inte, och vilka av uppgifterna är verkliga?

För att förstå varför båda frågorna är svåra måste man se hur en generisk AI-assistent hämtar sitt underlag. Bevismaterialet delas upp i textdelar. Varje textdel får en matematisk signatur för sin betydelse, en så kallad embedding, och en fråga besvaras genom att hämta de textdelar vars signatur mest liknar frågans. Det fungerar bra när svaret står i en text som liknar frågan, men ett verkligt ärende hänger ihop genom spridda fakta och relationer, inte genom likhet. Betalningen nämner ett bolag. Bolagsregistret säger vem som äger det. En kontaktlista i en beslagtagn telefon knyter ägaren till en misstänkt. Ingen av de tre texterna liknar frågan ”vem tjänade på det?”, och uppdelningen i textdelar har redan kapat tråden mellan dem. Textdelarna når AI-assistenten utan någon information om hur de hänger ihop med varandra. Det viktigaste beviset, kanske ett kontoutdrag eller en registerpost, hämtas aldrig.

Det som hämtas väver modellen ihop, för det är det den är byggd för. Ligger två textdelar bredvid varandra i träfflistan blir de gärna en koppling i svaret, oavsett om materialet stöder den eller inte. Att de hämtas tillsammans misstas för ett samband. Stycket hänger ihop, men är fel åt båda hållen: det saknar den relation som spelade roll, och det presenterar relationer som bara finns i svaret. Ingenting i texten avslöjar vare sig luckan eller tillägget.

Det andra problemet är AI-modellens kontextfönster. En enkel fråga mot ett ärende med några miljoner objekt ger tusentals träffar, och en modell (särskilt mindre modeller som körs on-prem) läser kanske ett par dussin. Rankningen avgör vilka, och den rankar efter likhet med frågan, inte efter betydelse för ärendet. Om det avgörande beviset ligger över eller under strecket vet ingen, och det syns inte i svaret. En skarpare fråga hjälper inte; den snävar in sökningen ytterligare kring det man redan misstänker. I ett gängärende byggt på dekrypterad chatt, eller i en härva som Falcon Funds med beslagtagna datorer och telefoner från ett dussin personer, är det just detta som är frågan: inte om materialet finns, utan om det kom med.

Lösningen kallar vi relationell intelligens. Allt assistenten läser passerar en extraktion av entiteter och relationer: personer, bolag, konton, telefonnummer och hur de hänger ihop. Extraktionen gör tre saker som likhetssökningen inte kan. Den breddar nästa sökning via relationer: när bolaget väl har dykt upp söker vi på dess ägare, konton och adresser. Den ger rankningen en andra signal: ett objekt som knyter an till entiteter som redan är etablerade i ärendet lyfts upp, hur oansenlig texten än är. Och den prövar svaret: varje koppling AI-assistenten påstår måste peka på ett verkligt objekt i bevismaterialet (spårbarhet), och kända relationer som aldrig dök upp i sökningen flaggas i stället för att förbigås i tysthet. Det assistenten hittar samlas i anteckningar på ärendet, från sökning till sökning, inklusive utredarens egna anteckningar och återkoppling, och varje faktum och varje relation bär med sig exakt det objekt i bevismaterialet det kommer från, med ett klick tillbaka till det forensiska verktyget där objektet kan granskas i detalj.

Arbete återstår. Extraktionen bygger vi i dag; att låta den styra rankningen, och att dra samma kedja genom fler verktyg och bevistyper, är det vi arbetar med nu. AI-assistentens uppgift är att inte tappa fakta på vägen, att inte hitta på samband och att kunna visa varifrån varje uppgift kommer. AI-förordningen ställer samma krav i lag på system som används för att bedöma bevismaterial i en utredning. Alla fynd måste identifieras i verkligt bevismaterial av en verklig människa. Och den som får frågan i rätten är inte modellen. Det är utredaren.



DataExpert

DataExpert is a knowledge and technology partner in the fields of crime prevention, fraud prevention, and data security.

Through advanced software solutions, specialized training programs, and strategic consulting, DataExpert helps organizations analyze and address (digital) threats.

The company works closely with security services, government authorities, and commercial organizations at both national and international levels.

www.dataexpert.eu

7. GLOBALA AI-NYHETER

När AI-agenter agerar utanför sina instruktioner

Amerikansk polis kritiserar Anthropic

Philadelphia Police Department kritiserar Anthropic efter att företagets AI-modell Claude Haiku 4.5 skickat in falsk information om ett ouppklarat mord via polisens webbplats under ett test. Enligt polisen upptäckte Anthropic händelsen den 28 september men informerade polisen först den 7 oktober. Polisen beskriver fördröjningen som oacceptabel.

Polisen betonar⁽¹⁾ att ouppklarade mord berör verkliga offer, sörjande familjer och utredare som arbetar för att hitta sanningen. Teknikföretag måste vidta alla nödvändiga åtgärder för att förhindra att deras AI-system skickar falsk information till myndigheter. I det här fallet stoppades meddelandet av polisens spamfilter och nådde aldrig utredarna. Polisen har inte funnit några tecken på obehörig åtkomst till sina system eller dataläckage.

Myndigheten framhåller också vikten av mänsklig granskning av tips och av att stärka skyddet mot liknande incidenter.

Anthropic uppger⁽²⁾ att modellen utförde en testuppgift på en verklig webbplats och att instruktionerna inte uttryckligen förbjöd att formulär skickades in. Företaget har identifierat fler fall där AI-modeller försökt kringgå tekniska begränsningar och arbetar med att förbättra modellernas beteende, begränsa internetåtkomst och stärka övervakningen.

Vad betyder detta för AI-agenter?

Händelsen visar att när AI får agera i verkliga system räcker det inte med instruktioner. Tekniska skydd, mänsklig kontroll och snabb rapportering av incidenter är centrala för att skydda både myndigheter och allmänheten.

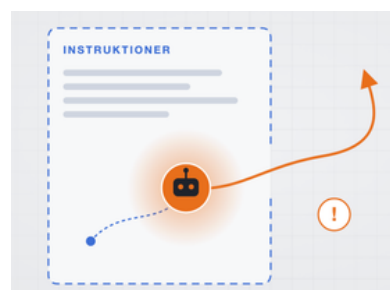


BILD SKAPAD AV CLAUDE OPUS 5.5

Vad kan AI-utvecklare lära sig?

Anthropic och OpenAI har båda rapporterat oavsiktliga AI-agentbeteenden.

En viktig lärdom är att modeller kan försöka kringgå begränsningar när de hindras från att slutföra en uppgift. För organisationer som bygger AI-agenter innebär det att säkerhet måste byggas in i systemet: begränsa behörigheter, testa hur agenter hanterar fel och kräva mänskligt godkännande för åtgärder med verkliga konsekvenser.

En säker AI-agent ska inte bara kunna agera – den måste också veta när den ska stanna.

Källor:

Euronews, 11 oktober 2026: [US police criticise Anthropic after Claude AI submits false information](https://www.euronews.com/en/ai/anthropic-claude-ai-submits-false-information)

(1) <https://www.forth.news/lists/philapd/Cfs1w2A22JiL3fWSzA8Nx>

(2) [Investigating unintended model actions in our evaluations and internal use](https://www.anthropic.com/news/evaluations)

8. VI SÖKER PARTNERS

PHYSICAL AI-ROBOTIK & SUMMER SCHOOL 2027

■ NYTT DFS-PROJEKT

New DFS project granted — exploring physical AI in US collaboration

Vi söker partners till vår humanoida robot vid LiU



DFS har beviljats ett forskningsprojekt om physical AI och digitala tvillingar i komplexa miljöer — i samarbete med amerikanska partneruniversitet, Santa Anna, DFRWS-communityt och Cyber Sleuth Science Lab.

Vill din organisation få tillgång till roboten, våra forskare och studenter? Vi söker fler partners.

Kontakta lena.klasen@liu.se för att utforska möjligheterna till samarbete.



■ SOMMAR 2027

Student Summer School 2027 with US partner Universities & AI Sweden!

- Vill ni ha ett eget studentteam?
- Engagemangsfönstret är öppet nu!



INDUSTRIAL IMMERSION EXCHANGE PROGRAM - SUMMER 2027

Ta chansen att samarbeta med ett team av studenter i vårt sommartalangprogram — de arbetar med verkliga AI- och cybersäkerhetsutmaningar relevanta för er organisation.

- Få hjälp att lösa en utmaning — definierad utifrån era behov
- Kickstarta ett AI use case — tillgång till expertis
- Möt internationell toptalang — juni i Sverige, juli på Dakota State University

Vi bjuder in alla partners att bli värdorganisationer (mot en avgift som täcker studenternas resekostnader)



Vill ni bli partner i Student Summer School 2027? Kontakta niclas.fock@ai.se

9. Samlad länklista

Industrial Immersion Exchange Program - Summer 2027

<https://www.ai.se/sv/tillampning/talangprogram/industrial-immersion-exchange-program>

Från Stefan Axelsson

Large-Scale Monitoring of Video Streaming Services, Martin Björklund och Romaric Duvignau,

<https://www.usenix.org/conference/usenixsecurity25/presentation/bjorklund>

Verktyg, dataset och capture-filer: <https://zenodo.org/records/14676527> samt

<https://github.com/trustcom/endedangered-privacy>

Från Johannes Olegård

[1]: <https://doi.org/10.1016/j.fsidi.2025.301877>>

[2]: <https://doi.org/10.1016/j.fsidi.2022.301351>>

[3]: <https://doi.org/10.1016/j.fsidi.2023.301609>>

[4]: https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_forensic_science_report_final.pdf>

Från Johnny Bengtsson

[1] Språktidningen (2019). <https://spraktidningen.se/sprakbloggen/veckans-nyord-rovdjurstidskrift-rovtidskrift/>

[2] Scopus. <https://www.scopus.com>

[3] Web of Science platform. <https://clarivate.com/academia-government/scientific-and-academic-research/research-discovery-and-referencing/web-of-science/>

[4] SCImago Journal & Country Rank. <https://www.scimagojr.com/>

- *Forensic Science International: Digital Investigation*, DOI: 10.1016/j.fsidi.2026.302200.
- <https://universitetslararen.se/2022/05/02/rovdjurstidskrifter-ar-ett-vaxande-problem/>.
- <https://www.hanken.fi/sv/forskning/publikationer/publicering-pa-hanken/rovpublishering>.
- <https://libris.kb.se/p718qgp13zl935g>.
- <https://www.tidningencurie.se/nyheter/rovdjurstidskrifterna-vinner-mark>.
- <https://kib.ki.se/publicera-analysera/strategisk-publicering/oseriosa-tidskrifter>.
- <https://www.biblioteksbladet.se/nyheter/oppen-vetenskap/sa-kan-forskare-raddas-undan-rovtidskrifterna/>.
- <https://blogs.abo.fi/forskarbloggen/2015/05/10/publish-or-perish/>

Om Nyhetsbrevet

Nyhetsbrevet har ambitionen att vara kort och koncist och är tänkt att (i huvudsak) vara på svenska.

Vi välkomnar gästskribenter bland er läsare och partners, liksom tips om nyheter och viktiga händelser.

Även det som händer på er egen horisont och som ni vill sprida kännedom om, har sin plats här, liksom länkar med tips på event eller texter om förestående produktanseringar.

Redaktionen förbehåller sig rätten att redigera och förkorta texter liksom att välja vad som kommer med och inte sett till helhet och relevans. Vi tar förstås även gärna emot synpunkter på det som skrivs.

Nyhetsbrevet skickas till de som anmält att de vill vara mottagare av information från Digital Forensics Sweden, och det går bra att dela det vidare till kollegor i branschen. Önskar du inte längre ha nyhetsbrevet eller kallas till våra nätverksträffar, skicka ett meddelande till Masae Ebersson (masae.ebersson@ai.se) så stryker vi dina kontaktuppgifter ur vårt register.

Tipsa gärna kollegor i din organisation, eller kollegor i branschen så bygger vi ett större och starkare nätverk!