



Digital Forensics Sweden

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

digital-forensics.se

NYHETSBREV

NR.13 / MAJ 2026

INNEHÅLL

1. Inledning — Niclas Fock
2. DFRWS EU 2026 — Konferens recap
3. Forskningsnytt — Johnny Bengtsson
4. Krönika — Stefan Axelsson
5. Forskningsnytt — Johannes Olegård
6. Nätverksträff
7. Flera länkar



NÄSTA NÄTVERKSTRÄFF

4e juni - [Spektrum](#), [Ebbepark i Linköping](#)

Tema: Det utvidgade hotlandskapet

Hotbilden mot samhälle, organisationer och individer har förändrats i grunden. Det räcker inte längre att skydda ett nätverk eller säkra en server-hoten rör sig idag över gränser vi tidigare tog för givna: mellan det fysiska och det digitala, mellan fred och krig, mellan verklighet och perception.

På den här träffen utforskar vi tre dimensioner av detta utvidgade hotlandskap- och vad de kräver av oss som arbetar med forensik och säkerhet.

Välkommen till ett nytt nyhetsbrev från Digital Forensics Sweden – det nationella initiativet för att öka kunskapen inom området Digital Forensik och knyta samman och gemensamt stötta samhällets alla aktörer som bekämpar en ökande cyber-brottslighet, men också nyttja ny teknologi för att utveckla framtidens metoder för digitala utredningar.

Året inleddes med att kulmen på lång tid av förberedelser nåddes när vi i Linköping genomförde den största konferensen inom DFRWS (Digital Forensics Research Workshop) mångåriga internationella historia, och för första gången någonsin i Sverige – läs mer om konferensen i nyhetsbrevet. Artiklar från konferensen finns publicerade här:

<https://dfrws.org/presentation/>

Digital Forensics Sweden har också fått finansiering för ett nytt projekt genom Vinnova/Avancerad Digitalisering. En ansökan som letts av Lena Klasén, tidigare Polisen och initiativtagare och co-director till Digital Forensics Sweden. Projektet är en logisk fortsättning på våra tidigare projekt kring brottsplats-visualisering, nu i ett utökat konsortium med fler av er nätverkspartner medverkande.

Projektet hanterar sömlöst data över stora områden från satellit till inomhusmiljöer, kombinerar generativ agentisk AI med visualisering av brottsplatsdata, och skapar nya metoder för digitala utredningar som också kan ha tillämpning i exempelvis krisledning. Vi kommer att få anledning att återkomma till projektet som kommer att löpa under två år.

Jag vill passa på att upmana er att anmäla er till vår kommande nätverkstärff den 4/6 i Linköping, om ni inte redan gjort det.

I detta nummer kan ni också läsa vår återkommande skribent, professor Stefan Axelssons reflektioner kring Mythos, samt ta del av nyheter från några av de forskare inom digital forensik som skriver i nyhetsbrevet.

Håll tillgodo!
Niclas Fock

2. DFRWS EU 2026 – STORT GENOMSLAG I SVERIGE !

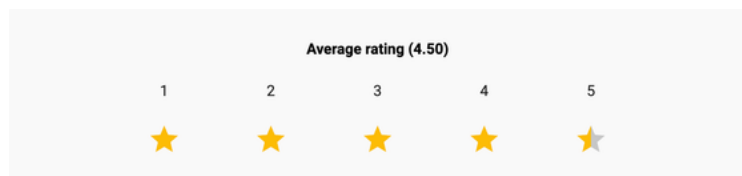
The Digital Forensics Research Konferens (DFRWS EU 2026) arrangerades den 24 till 27 mars i Linköping, och sista dagen i Norrköping. Eventet organiserades i samarbete med LiU och Digital Forensics Sweden.

Efter nästan 1 år av intensiva förberedelser blev DFRWS EU 2026 en succé under vecka 13.

Ca. **240 deltagare på plats och 50 online, från mer än 50 länder** - fler än någonsin tidigare.

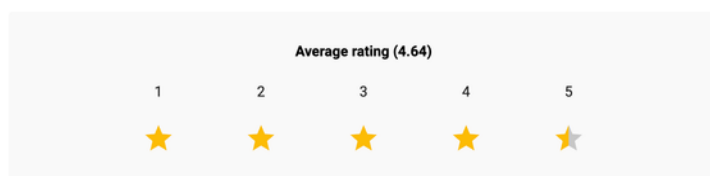
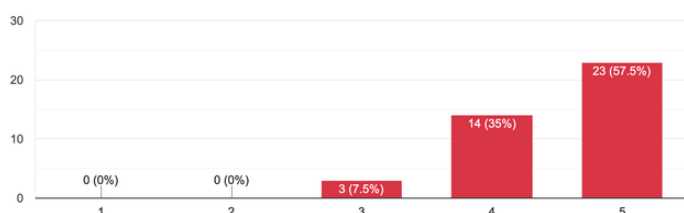


Enkätsvaren visar det sig att även **nöjdheten var rekordhög** - det säger nog det mesta om veckan!



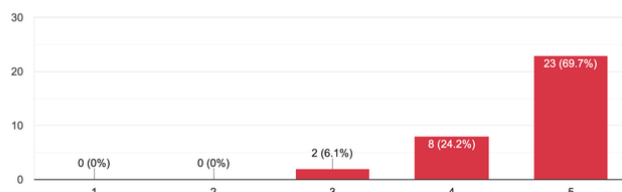
How would you rate the conference overall?

40 responses



Please rate the evening events (welcome reception, banquet and networking events)?

33 responses



Konferensöversikt

MÅNDAG

Konferensveckan inleddes med workshops för Women in Forensics Computing (**WinFC**) och **Project VIC** (avancerad teknik för att bekämpa sexuell exploatering av barn och människohandel). — följt av Women in tech industry mingle och kickoff för ett tvådagars Rekryteringsevent (SAAB, FOI, Polisen, Combitech & AI Sweden) på kvällen.

TISDAG

4 parallella workshops inkl. **Digital Forensics Doctoral Symposium** tog vid när delegaterna anlände. På kvällen hölls välkomstreceptionen med tal av **Erika Skoogh**, biträdande enhetschef på Nationellt forensiskt centrum, Polisen — och underhållning av Linköpings universitets manskör!

ONSDAG

Dagen inleddes med **en morgonlöpning** ledd av en löpleddare från NFC, där deltagarna fick en energifylld start på dagen och möjlighet att uppleva Linköpings vackra natur. Konferensen fortsatte med en keynote “Visions of Digital Policing” av **Heidi Mork Lomell** - professor vid Universitetet i Oslo, följt av ett flertal paper sessions inom områden som Memory Forensics, Mobile Device Forensics och AI in Digital Forensics.

På kvällen: Bankett på Flygvapenmuseum med Årets Rodeo — ett fiktivt fall med ett försvunnet flygplan över Östersjön.



Torsdag

Keynoten “The Need for Forensics in the Age of Hybrid Warfare” av Emil Hjalmarson från FOI (Totalförsvarets forskningsinstitut) engagerade deltagarna och ledde till många intressanta frågor. Feedback från en av deltagare: “A very nice comparison and overview of current events and developments around the world, with a focus on digital forensics.”

Därefter genomfördes postersessioner samt fler presentationer.

DFRWS EU 2026

FREDAG — MULTIMEDIA FORENSICS I NORRKÖPING

Avslutningsdagen på Visualiseringscenter C bjöd på ett helt eget spår för Multimedia Forensics.

Dagen inleddes med tal av **Anna Sotkasiira Wik** (ordförande i Kommunfullmäktige/Borgmästare, Norrköpings kommun) och **Rikspolischef Petra Lundh**, som även deltog i lanseringen av **“Interactive Digital Twin”** som ett forensiskt verktyg med hjälp av multimodal AI vid digitaliserade brottsplatser. Dagen avslutades med en guidad tur i Open Space ledd av professor **Anders Ynnerman** och Guidad stadsvandring.



Rikspolischefen: Utvecklingen inom digital forensik är avgörande

- Rikspolischef Petra Lundh höll ett anförande. Hon lyfte den stora förändringsfas som europeisk brottsbekämpning befinner sig i, där polisen behöver anpassa sig till en brottslighet som är mer omfattande, mer internationell och mer tekniskt avancerad än tidigare.
- En central del i förändringen är att utveckla en mer informationsdriven brottsbekämpning där vi är bättre på att samla in, tillgängliggöra, analysera och värdera information, sa Petra Lundh och poängterade den viktiga roll som it-forensiken spelar.
- Hon talade om hur viktigt det är att brottsbekämpningen är internationell, i och med att den organiserade brottsligheten är det. Och hur avgörande det är med samverkan.
- Petra sa också att samarbete mellan myndigheter, mellan länder och mellan offentliga och privata aktörer är helt nödvändigt för att vi ska kunna möta dessa utmaningar. Den konferens som har hållits här denna vecka är ett mycket bra exempel på detta. Den visar hur viktigt det är att dela kunskap, erfarenheter och idéer.

Ett stort tack till alla deltagare, team och sponsorer som gjorde det möjligt!

Nästa år, DFRWS EU 2027 arrangeras i **Edinburgh, Skottland** 30 mars -2 april, 2027.

Mvh,
Niclas Fock (Local chair), Masae Ebersson (Local co-chair), Maria Holmkvist (Local co-chair), Lena Klasén (Session chair), Stefan Axelsson (Rodeo chair) & Daryl Pfeif (Styrelseledamot)

MSAB

DataExpert

AMPED
SOFTWARE



NORRKÖPINGS
VISUALISERINGSCENTER

NORRKÖPING

PROJECT VIC
International

Linköping
Där idéer blir verklighet

AI
SWEDEN

santa anna

Li.U
LINKÖPINGS UNIVERSITET

Inledning

I det förra nyhetsbrevet berättade jag om pausen i min forskning. Denna paus gäller dessvärre tills vidare. Inte för att jag inte vill eller på grund av lathet; det är de som står mig nära som måste prioriteras. Dessa är just nu betydligt viktigare än forskning.

I de flesta fall anser jag att det viktigt att kunna förmedla resultatet av en offentligt finansierad verksamhet, då det direkt eller indirekt är du och jag som bekostar denna. Nu är jag inte direkt en person som söker uppmärksamhet eller bekräftelse, men gläds åt att få ett slags erkännande av de som ser den praktiska nyttan ens arbete. Detta gjorde bland annat IoT-evangelisten Ulf Seijer, som valde att uppmärksamma min forskning genom sin artikel i Elektroniktidningen [1]. Detta gav lite oväntat fler ringar på vattnet [2],[3]. Nu inser förhoppningsvis fler att insamlad data även kan användas i en brotts- och brandutredande kontext.

Sedan var det ju det där med it-forensik och brandutredningar, alltså den övergripande metodiska process som syftar till att besvara alla frågor som exempelvis innefattar brandorsak, brandförlopp, tillvägagångssätt, tänkbara utförare med mera. Tanken på att vidareutveckla området är inte släppt, utan ligger latent i bakhuvudet. Relaterat detta är en artikel som mina medförfattare och jag fick publicerat i Forensic Science International [4]. Manuskriptet till artikeln har jag valt att bygga vidare på utifrån en konceptuell poster som presenterades förra året på EAFS 2025 [5].

Men nyfikenheten tar inte stopp där. Jag har några idéer på hur it-forensiken ska kunna tas vidare inom området additiv tillverkning, något som jag har berättat om i tidigare nyhetsbrev. Sedan ett tag tillbaka har jag ägnat tid åt hur en generell metodik skulle kunna se ut och som syftar till att utifrån funna artefakter som G-code-filer, 3D-modeller och traditionell it-forensik knyta samman dessa. Tanken har väckts utifrån ett ärende som var tänkt att gå upp i hovrätten, men där både den dömde och åklagaren nöjde sig med tingsrättsdomen. Jag kanske utvecklar tanken vid något annat tillfälle.

Till dess, njut av våren/försommaren!

Johnny, NFC

Källor

[1] Seijer, U. (2026). IoT-data som bevis i brottsutredningar. Elektroniktidningen 1-2/2026.

[2] Höckerbo, S. (2026). Sensorer kan bli nya vittnen i brottsutredningar.

<https://liu.se/nyhet/sensorer-kan-bli-nya-vittnen-i-brottsutredningar>

[3] Engberg, J. (2026). Din luftkonditionering kan lösa brott – forensikern berättar hur.

<https://www.sverigesradio.se/artikel/din-luftkonditionering-kan-losa-brott-forensikern-berattar-hur>

[4] Bengtsson, J. et al. (2026). Integrating digital forensics into fire scene investigation: Enhancing reconstruction and analysis. DOI: 10.1016/j.forsciint.2026.112924

[5] EAFS 2025 (2025). Best Poster Presentation Award. <https://eafs2025.org/best-poster-presentation-award/>

Mythos och Cyberforensik

Jag håller kursen i cyberforensik så här års, och det leder naturligt tankarna på hur området utvecklas. Alla pratar naturligtvis om LLM:er hela tiden, det är nästan så man blivit lite uttråkad, men det går tyvärr inte att undvika att tänka på hur dessa kommer att påverka även det här området.

Då kommer vi naturligt in på Claude Mythos Preview, och vad den ställer till med. Alla har väl hört om den nu, men som snabb sammanfattning så har alltså Anthropic utvecklat en ny modell som man hävdar är så kapabel inom cybersäkerhetsområdet att man inte släpper den öppen utan att stora aktörer fått en chans att säkra upp sina system först. Detta genom Project Glasswing. Mycket har sagt om hur duktig Mythos är på att hitta nya zero day svagheter, och det är inte bara Anthropic som säger det. Mozilla Foundation rapporterar till exempel att förra modellen, Opus 4.6 hittade 22 systemsvagheter i Firefox 148, men Mythos hittade hela 271 svagheter i Firefox 150. Så antingen har Mozillas programmerare blivit mycket sämre på kort tid, eller så har Claude blivit mycket bättre. De smarta pengarna får väl ändå sägas ligga på det senare.

Men, vad jag själv tycker är mera intressant, och något som kommer att få större inverkan på själva forensiken, är rapporterna om hur mycket bättre Mythos är på att faktiskt utnyttja svagheter, snarare än att bara hitta dem. Detta är också en förmåga som gått fram med stormsteg på bara det senaste året och här får vi också lite mer kött på benen från Anthropic. De förklarar i detalj hur Mythos lyckas utnyttja redan kända svagheter i Linux kärnan, svagheter som ingen egentligen trott varit särskilt allvarliga. Det är klart att de varit identifierade som svagheter, men ingen har egentligen sett att det funnits någon anledning till oro eftersom de mera rört sig om skönhetsfläckar, med exempelvis något marginellt dataläckage (i storleksordningen en byte eller så) snarare än en lätt utnyttjad allvarlig svaghet. Men för Mythos så är det allt som behövs. Genom att sy ihop en tre, fyra, olika sådana svagheter, och genom att använda dem i en kedja med dussintalet steg, så lyckas den gå hela vägen till totalt brott mot säkerheten.

Så nu ser vi första tecknen på övermänsklig förmåga. Inte i termer av att Mythos skulle vara superintelligent och göra saker som ligger helt bortom mänsklig fattningsförmåga (som i science-fiction dystopierna), utan helt enkelt genom att operera på topp av mänsklig förmåga (eller strax under) men genom att kunna göra det mycket längre och snabbare än vad en människa, eller ett team av människor, skulle rimligtvis kunna orka med. Som Jan Freese, tidig direktör för datainspektionen, insåg redan på sjuttioalet; datorer tar bort manuella spärrar. Dvs de möjliggör det som tidigare var teoretiskt möjligt, men praktiskt omöjligt. Med Mythos så blir det helt plötsligt realistiskt att hitta dessa oerhört tillkrånglade sätt att kombinera många små missar till en stor dito. Något som förut var möjligt i teorin, men praktiskt ogenomförbart.

Så lägstanivån höjdes helt plötsligt ett antal steg. Andrummet försvann och sannolikhetskalkylen förändrades. Det som förut var möjligt men otroligt, blir i en nära framtid snarare oundvikligt. Man kan inte kalla något "låg risk" längre.

Och detta kommer att få stor påverkan på utredningen av dessa penetrationer. Även om det ofta kan vara enklare att följa i någon annans fotspår än att vara den som först stakar ut vägen, så känns den ändå som att utredare i framtiden kommer att behöva vara lika välutrustade med LLM:er som angriparna kommer att vara. Det kommer att ta alldeles för lång tid att återskapa dessa komplicerade och långa intrångskedjorna annars.

Nu sker det som tur är lite forskning inom just det området. LLM:erna lockade med fördelar även innan de kanske blev nödvändiga. Det finns forskning om hur LLM:er skall användas för att exempelvis leta igenom loggmateriel osv., men intressant nog så hittar jag ingen forskning om att använda dem i andra änden. Nämligen som hjälp för att sätta upp sitt system så att dessa angrepp har en chans att bli upptäckta. Det är nämligen inte alls omöjligt att be en LLM att när den ändå håller på och hitta en väg in i systemet, också tänka på hur den skall undgå upptäckt. Det kanske tar några tiotalas, eller hundratals steg för att göra det, men det är en smal sak för en LLM att fundera på, och genomföra. Den har ändå inget annat bättre för sig. Så även där riskerar vi att en manuell spärr försvinner, och det kan komma att få stor påverkan. Forensic readiness, dvs att redan innan angreppet fundera på vilka spår man skulle vilja ha när det värsta händer, kommer att bli ännu mera aktuellt och oundgängligt.

Så slutligen så håller jag med de som tror att sett till helheten så är nog de här nya förmågorna i längden mest till hjälp för försvararna. Som försvarare så måste man ju som bekant försvara överallt, medan angriparen bara behöver hitta en väg in och kan koncentrera sig på denna. Med LLM:er så blir jobbet att försvara överallt inte lika oöverskådligt och praktiskt omöjligt som tidigare. Jämför just Project Glasswing när man försöker ge försvararna en chans att komma in i matchen på allvar innan angriparna får beträda arenan. Men det gamla sättet att göra saker på kommer nog inte att överleva. Vi kommer att behöva göra och tänka nytt, och det ganska omedelbart. Att det antagligen är positivt i längden hjälper inte de nödvändigtvis här och nu.

Mina Kinesiska kollegor berättar att det inte finns någon gammal Kinesisk förbannelse som lyder "Må du leva i intressanta tider." De hade inte hört talas om det uttrycket innan de kom till väst. Men de håller samtidigt med om att det låter som en gammal Kinesisk förbannelse, och att de borde ha haft den. Så oavsett vem som myntade det, kan vi i alla fall konstatera att vi nu lever i intressanta tider. Mycket intressanta tider...

Källor

Anthropics offentliggörande av Claude Mythos Preview och dess inverkan på cybersäkerhet. Värld att läsa i sin helhet:
<https://red.anthropic.com/2026/mythos-preview/>

Anthropics presentation oav Project Glasswing:
<https://www.anthropic.com/glasswing>

Mozillas berättelse av hur Project Glasswing har påverkat Firefox:
<https://blog.mozilla.org/en/firefox/ai-security-zero-day-vulnerabilities/>

5. Forskningsnytt

Johannes Olegård

I thought I would highlight some interesting articles that have popped up recently:

"The implementation of digital forensic science in a Swiss police force",

<https://doi.org/10.1016/j.fsidi.2026.302069>

Some statistics from a Swiss forensics unit---including some interesting observations about things going wrong.

"Cybercrime investigations in practice: Insights from the LockerGoga ransomware attack on Norsk Hydro", <https://doi.org/10.1016/j.fsidi.2026.302111>

While the paper talks a lot about a certain framework, it's interesting to read about the case itself and how it was handled.

"Plug to place: Indoor multimedia geolocation from electrical sockets for digital investigation", <https://doi.org/10.1016/j.fsidi.2026.302056>

Image recognition of wall sockets to geolocate photos. I just thought that was neat for something so simple. (Note that this paper was presented at DFRWS 2026 EU in Linköping).

6. Nästa nätverksträff

4e juni kl.09.30 - 16.00

Agenda

09:30 - Registration and coffee at [Fridtunagatan 41, Spektrum](#) Ebbepark in Linköping

10:00 - Welcome by RISE

10:10 - Network information / Update

10:25 - WASP WARA-PS, a research arena in development

Jesper Tordenlid, Combitech and responsible for WARA-PS

10:55 - **Key Note #1:** "The need for forensics in the age of hybrid warfare"

Dr Emil Hjalmarsen (FOI)

12:00 - Lunch

12:50 - **Key Note #2:** "Digital forensics aspects of 3D-printing technology"

Johnny Bengtsson, Police/NFC

13:35 - **Key Note #3:** "Expanding Threat Landscapes - Growing Needs for Cybersecurity and Forensics": Catharina Sandberg, LEAD

13:55 - Introduction to the Work shop

14:00 - **Work shop** on "The expanded threat landscape"

15:00 - Coffee

15:30 - **Key Note #4:** "Mythos presentation" Prof Stefan Axelsson

16:00 End

Om din kollega ännu inte är medlem men gärna vill delta i detta event, kontakta Niclas.fock@ai.se

7. Flera länkar

- Digital Forensics Sweden, vår egen site: <https://www.digital-forensics.se>
- Anthropics offentliggörande av Claude Mythos Preview och dess inverkan. på cybersäkerhet. <https://red.anthropic.com/2026/mythos-preview/>
- Anthropics presentation oav Project Glasswing: <https://www.anthropic.com/glasswing>
- Mozillas berättelse av hur Project Glasswing har påverkat Firefox: <https://blog.mozilla.org/en/firefox/ai-security-zero-day-vulnerabilities/>
- EAFS 2025 (2025). Best Poster Presentation Award: <https://eafs2025.org/best-poster-presentation-award/>
- Höckerbo, S. (2026). Sensorer kan bli nya vittnen i brottsutredningar <https://liu.se/nyhet/sensorer-kan-bli-nya-vittnen-i-brottsutredningar>
- Engberg, J. (2026). Din luftkonditionering kan lösa brott – forensikern berättar hur. <https://www.sverigesradio.se/artikel/din-luftkonditionering-kan-losa-brott-forensikern-berattar-hur>
- "The implementation of digital forensic science in a Swiss police force", <https://doi.org/10.1016/j.fsidi.2026.302069>
- "Cybercrime investigations in practice: Insights from the LockerGoga ransomware attack on Norsk Hydro", <https://doi.org/10.1016/j.fsidi.2026.302111>
- "Plug to place: Indoor multimedia geolocation from electrical sockets for digital investigation", <https://doi.org/10.1016/j.fsidi.2026.302056>

Vill din organisation eller ditt företag synas i vårt nyhetsbrev?
Nyhetsbrevet riktar sig till våra medlemmar och är även öppet för allmänheten online.
För annonsering och samarbetsmöjligheter, kontakta niclas.fock@ai.se

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 produktlanseringar.

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!