DIGITAL FORENSICS SWEDEN

NYHETSBREV

NR.12/ OKT 2025

Innehåll

1. Inledning - **Niclas Fock**
2. Forskningsnytt: *"Brandrestprovet, den fula ankungen och 3D-skrivaren"* - **Johnny Bengtsson**
3. Krönika: *"AI lögner och om det går att hitta dem"* - **Stefan Axelsson**
4. DFRWS Konferens 2026 i Linköping - Info om sponsorskap
5. Nästa Nätverksmöte
6. Event: **Games for Change** IDT Multimodal AI projekt
7. Flera länkar

Nästa nätverksträff

Den 26 november
kl.09:30–16:30
MSAB i Stockholm

Tema: Attacker mot samhällets infrastrukturer

Dagen innebär också att vi får stifta närmare bekantskap med MSAB:s verksamhet.

1 Inledning

Niclas Fock

Välkommen till ett rykande färskt nyhetsbrev från Digital Forensics Sweden!
Vi brinner för att utveckla Sveriges förmåga att utreda och lösa brott i den digitala eran. Genom den extremt snabba utvecklingen inom AI ser vi dagligen nya exempel på brott och allt allvarligare hot mot samhället, ett skeende där vi vill kraftsamla Sverige och alla som ni som ser det här som en av vår tids viktigaste uppgifter.

Centralt för att kunna verka långsiktigt, är en grundfinansiering, något vi strävat efter under de dryga sju år vi har verkat. Vi ser ljuspunkter, men tyvärr också bakslag i det arbetet. Viktigast är att vi inte ger upp. Tyvärr har vi inte fått vår ansökan hos Vinnova om en förstudie för ett Excellenskluster. Detta utesluter inte att vi ändå kan söka medel för Excellenskluster, men det innebär förstås en tuffare resa; endast fem kluster kommer att beviljas medel av Vinnova.

Parallellt jobbar vi på andra ansökningar där den mest omfattande är en ansökan om ett strategiskt forskningsområde, en ansökan som drivs at Linköpings Universitet för hela området Forensiska vetenskaper. Med i ansökan är även Stockholms Universitet. Forskningsmedel är oerhört viktigt, men ger inga stärkta förutsättningar för driften av Digital Forensics Sweden. Vi kommer därför att under 2026 att introducera en enkel partnermodell med (låga) medlemsavgifter för att fortsatt kunna driva arbetet framåt, vi återkommer kring detta.

Positiva nyheter är förstås att vi rusar mot mars och konferensen DFRWS 2026 (EU)! Här har vi fått flera sponsorer som självmant hört av sig, men vi behöver verkligen er partners nu – så riktat till både företag och myndigheter i nätverket: Se detta som en fantastisk möjlighet att exponera er verksamhet för nyckelpersoner inom området, eller kanske som ett sätt att rekrytera – det kommer exempelvis erbjudas möjlighet att möta studenter och forskare -men också som ett viktigt sätt att visa ert stöd för det oberoende och icke-vinstdrivande Digital Forensics Sweden – det helsvenska initiativet för att bygga ett Sverige mer motståndskraftigt mot brott i den digitala eran.

I detta nummer får ni läsa intressanta artiklar och kåserier av våra trogna skribenter, Stefan Axelsson (Stockholms Universitet) och Johnny Bengtsson (NFC/Linköpings Universitet).

Vi vill också uppmärksamma er på den kommande nätverksträffen hos MSAB i Stockholm den 26/11!

Trevlig läsning!

2. Forskningsnytt

Johnny Bengtsson

Inledande reflektioner

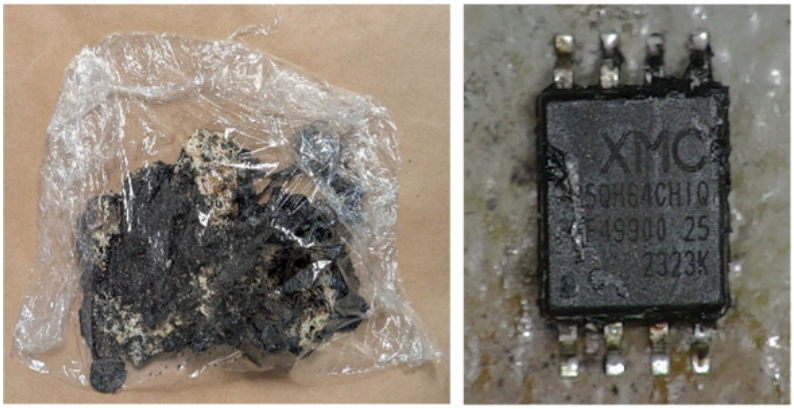
Sedan halvårsskiftet är mina forskarstudier satt på paus, inklusive forskningsprojektet som syftar till att tillvarata sensordata från fastighetsautomationssystem, vilket jag har valt att benämna fastighetsautomationsforensik. Min förhoppning är att jag på ett eller annat sätt kan få möjlighet att slutföra min licentiatuppsats under våren 2026.

Det har emellertid inte hindrat mig i att klura på andra verksamhetsnyttiga idéer som förmodligen går att bedriva forskning på, tankar som även finns med i tidigare nyhetsbrev [ref. 1, 2]. Dessa har kretsat kring att 1) försöka etablera it-forensik som ytterligare ett redskap vid brandplatsundersökningar och 2) kunna förstå hur it-forensik och skiktröntgen-utrustningar kan vara till gagn för forensiska analyser av 3D-skrivare och 3D-utskrivna objekt.

Brandrestprovet, den fula ankungen

Beträffande 1), så fick NFC för ett tag sedan in ett så kallat brandrestprov, en bränd klump som påstods utgöra rester av en webbkamera. Frågeställningen var här om det fanns något minneskort i den brända klumpen och om det i så fall skulle gå att rädda sparad data. Brandrestprovet såg initialt ut som ett hopplöst fall. För någon som inte är tillräckligt nyfiken skulle ett avfärdande från NFC:s sida lätt kunna tas med en axelryckning. En bränd klump är en bränd klump – men för att kunna hålla ryggen helt fri, så genomfördes en röntgengenomlysning med vår skiktröntgen. En sådan kan riskeras övergå i en ”skitröntgen” om man handlar fel, som att kontaminera en jättedyr utrustning med konduktiva sotpartiklar.

För att skydda innanmätet från sådana sotpartiklar virades brandrestprovet in i plastfolie (Figur 1, vänster), något som bekant används för att plasta in mat. Genomlysning visade visserligen att det inte fanns något minneskort i microSD-korthållaren. Däremot gick det att identifiera något som såg ut som en intakt minneskrets. Här togs beslutet att ta det ett steg längre än frågeställningen genom att frigöra minneskretsen för att undersöka möjligheten till datautläsning (Figur 1, höger).



Figur 1. Vänster: Brandrestprov som påstods utgöra en övervakningskamera. Höger: Frilagd minneskrets vars innehåll sedermera

Friläggningen gick bra, minneskretsen isolerades och utläsning av dess data gick utmärkt. Därefter tog några kollegor med mer luft i systemet sig an att analysera minnesinnehållet.

Resultatet visade att den fula ankungen ändå blev en sorts svan; ett bekräftade att datainnehållet representerade kamerans firmware som sedermera analyserades. Detta påvisar det tidigare gjorda påståendet att it-forensik kan vara till hjälp vid en brandutredning. Som dubbelt syfte kan denna erfarenhet utgöra ett underlag till avhandlingen genom exempelvis ett manuskript, vilket jag kanske utvecklar mer i något kommande nyhetsbrev.

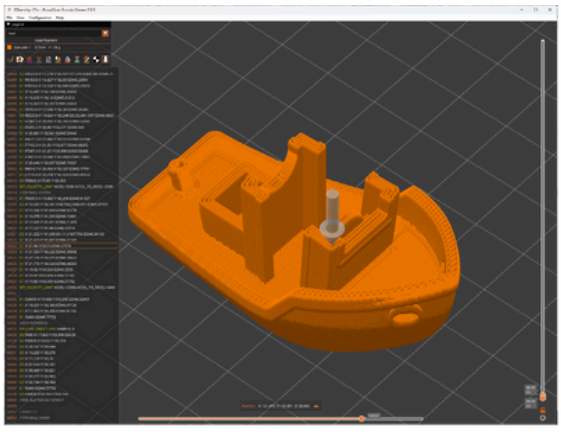
3D-skrivare

Gällande 2), så ser NFC en ökande trend i det som till vardags kallas 3D-vapen – eller 3D-utskrivna vapendelar, för att vara mer korrekt. Det ska i sammanhanget sägas att mängden vapenundersökningar i Sverige till största del utgörs av konventionella vapen, men även modifierade startpistoler, gasvapen, m.m. 3D-vapensituationen ser förmodligen annorlunda ut i olika länder och jurisdiktioner. Däremot

Mina tidigare tankar om 3D-skrivarteknologin, eller additiv tillverkning, har i någon mening infriats. NFC har i två skilda ärenden fått in 3D-skrivare för undersökning, där frågeställningarna har varit tämligen likartade: har det beslagtagna objektet X skrivits ut med 3D-skrivaren Y?

Även om NFC återigen gräver på okänd mark, så är angreppssättet för en it-forensisk undersökning likartat även här. Hypotesen om att skrivarmodellerna kan betraktats som inbäddade system med operativsystem och internt icke-flyktigt lagringsmedium stämde. Ur båda skrivarna extraherades en mängd filer som tidsmässigt indikerar på tidstämplade utskriftsaktiviteter, men framförallt G-code-filer och tillhörande tumnagelbilder av 3D-objekten som har hanterats av skrivarna.

En G-code-fil är resultatet av den process som benämns slicing och som sker med en slicerprogramvara. Syftet är att omvandla ett generellt 3D-objekt till en uppsättning specifika utskriftsinstruktioner för en särskild 3D-skrivarmodell. Instruktionerna innefattar bland annat objektet som sådant, dess orientering relativt utskriftsbädden, stödstruktur, utfyllnadsmönster och mönstrets densitet och lagertjocklek. Med hjälp av en G-code-simulator går det också att visualisera det objekt som ska skrivas ut (Figur 2). Ur ett utredningsmässigt perspektiv fanns det emellertid inte något behov av att göra någon volymrekonstruktion för att jämföra dessa med G-code-filerna. Detta kan dock vara av intresse att gräva vidare i framtiden. Detta kanske jag utvecklar vid något annat tillfälle, om sådant ges.



Figur 2. Visualisering av en G-code-fil med hjälp av PrusaSlicer G-code Viewer. Denna visar utskriftssekvensen för en 3DBenchy, en de facto-standardmodell för att testa den aktuella 3D-skrivaren.

Intryck från europeiska brottsbekämpande myndigheter och akademin

Under den här perioden har jag också hunnit med lite omvärldbevakning. I slutet av september blev jag inbjuden till Bratislava för att presentera it-forensiska aspekter beträffande 3D-vapen vid One day-One topic-Seminar (OOS) on 3D-printed firearms [3] och som arrangerades av ENFSI EPGT Working Group [4]. Deltagarna vid OOS:et utgjordes till största delen av experter inom den egna arbetsgruppen, men även några vapenundersökare, däribland en erfaren vapenundersökare från NFC och som också var mitt resesällskap. Fokuset för detta OOS var att samla olika forensiska discipliner under samma tak. Det jag tar med mig från heldagsseminariet är att det i kontexten 3D-vapen främst har fokuserats på traditionella vapenundersökningar, spårjämförelser samt kemiska analyser av filament.

Att 3D-skrivarundersökningar ännu inte har nått den etablerade it-forensiska communityn blev jag också varse om på det årliga ENFSI FITWG-mötet [5, 6] som i år arrangerades i Istanbul, där jag gav en snarlik presentation som den på OOS:et i Bratislava – men då med ett fördjupat it-forensiskt fokus, då expertisen in FITWG betonas på it-forensik. Både som forskningsämne och tillämpad it-forensik. Den stora vinsten med att nätverkandet vid sådana möten är möjligheten att stämma i bäcken. Vad finns det för behov och vad har (ännu inte) gjorts av andra?

Min samlade bedömning av de tre tidsmässigt närliggande eventen EAFS 2025 (beskrivet i [2]), ENFSI EPGT WG OOS och ENFSI FITWG är att it-forensiken i kombination med additiv tillverkning ännu är i sin linda. Det finns visserligen ett par it-forensiska publikationer kring detta, men fokuset är främst betonat på slicingprocessen som vanligen sker med en dator och inte underökning av 3D-skrivare specifikt. Här finns således en stor utvecklingspotential för fortsatta studier.

Avslutningsvis vill jag passa på att tacka Jyrki Juntunen (NFC) för att jag har fått låna hans ögon.

Johnny Bengtsson

Referenser

[1] Bengtsson, J. (2025), 6. Forskningsnytt #3. Digital Forensics Sweden, Nyhetsbrev No. 10, mars 2025.
[2] Bengtsson, J. (2025), 3. Forskningsnytt, Digital Forensics Sweden, Nyhetsbrev nr. 11, juni 2025.
[3] ENFSI EGTP WG (2025), One day-One topic-Seminar on 3D-printed firearms. https://enfsi.eu/news/epgt-successfully-organised-the-oos-on-3d-printed-firearms/
[4] European Paint, Glass & Taggants Working Group (2024), Paint, Glass & Taggants. https://enfsi.eu/about-enfsi/structure/working-groups/paint-glass-taggants/
[5] FITWG Istanbul 2026. https://fitwg.istanbul/event/day1/
[6] Forensic Information Technology Working Group (2012), The Forensic Information Technology (FIT) Working group interest. https://enfsi.eu/about-enfsi/structure/working-groups/information-technology/

3. Krönika

Stefan Axelsson

- AI lögner och om det går att hitta dem

Det är den tiden efter semestern när examensarbetarna som inte hann med under våren försvarar sina rapporter. I år så har en av mina studenter studerat en fråga som alltid varit intressant i alla utredningar, nämligen om någon ljuger. Idag så använder vi ju dock datorer för att ljuga; ingen har ju missat alla rapporter om deepfake; både video och ljud.

En fråga det inte talas lika mycket om i det övriga samhället är text. Det är en fråga som mycket stannat inom universitetsvärldens väggar. (Det pågår idag ett stort arbete med att anpassa universitetet till stora språkmodeller och frågan om det faktiskt är studenten som gjort det här arbetet eller inte.)

Så en av mina studenter, Xiaochun Li bestämde sig för att testa om dagens verktyg för att upptäcka fejk-text, något som blivit allt vanligare i olika försök till phishing, bedrägeri, spam och dylikt.

Så, kan vi detektera dessa genom att i alla fall i första läget, säga att de är skrivna av en LLM?

Så Xiaochun bestämde sig för att testa tre populära detektionsverktyg:
GLTR, DetectGPT, och ZeroGPT. De är bland de mest omtalade detektorerna idag.
GLTR (the Giant Language Model Test Room) är ett forskningsverktyg som flaggar ord i en text som rent statistiskt är "för förutsägbara." DetectGPT tar ett mer matematiskt tillvägagångssätt genom att "putta" en mening lite och se om den fortfarande passar modellens logic. ZeroGPT sist är det kommersiella verktyget; det är en svart låda i form av ett webverktyg som lovar nästan perfekt prestanda till varje som laddar upp suspekt prosa.

Så i studien så skapade Xiaochun ett balanserat dataset genom att använda flera olika källor inklusive egen generering av meddelanden, där hälften var skrivna av människor och hälften genererade av LLMer. Teman för texterna rörde sig över områden från finansbedrägerier till "Du har vunnit ett pris!"-meddelanden. Sedan så släpptes detektorerna lösa.

Resultatet blev ganska intressant. På pappret så ser ZeroGPT oslagbar ut. I reklamen så lovar de 98% "accuracy." (Ja, jag vet att det finns svenska termer, men de används så sällan i mina sammanhang, att jag tyvärr gett upp...) I utvärderingen så såg det dock inte alls lika bra ut. Den fick perfekt "precision" dvs den anklagade aldrig falskeligen en människa för att vara en AI, men detta på bekostnad av att bara korrekt identifiera 18% av de AI-genererade meddelandena ("recall").

Så den fångade några AI-genererade meddelanden, men de flesta slapp igenom.
Det är för övrigt vad man kan vänta sig av alla detektorer. Ju känsligare de är, desto färre slipper igenom, men desto fler falsklarm får man, och vice versa. Här har man uppenbarligen satt känsligheten för lågt för det här testfallet.

GLTR levererade istället ett mer balanserat resultat med 78% "accuracy" och "recall", med DetectGPT hack i häl med 71%. GLTR klarade medellånga meddelanden (tänk phishing email) medan alla detektorerna gjorde sämre ifrån sig på korta meddelanden, tänk SMS bedrägerier, antagligen för att dessa texter är för korta för att innehålla tillräckligt med information för att man, ens i teorin skall kunna klassificera dem rätt. Intressant var att detektorerna tycktes göra bäst ifrån sig på medel-långa texter. Blev de för långa så sjönk prestandan, eventuellt för att texterna då innehåller för mycket "brus" som förvirrar detektorerna.

Historien slutar dock inte där, utan Xiaochun testade sedan att modifiera meddelandena för att göra dem svårare att detektera; på samma sätt som en angripare skulle kunna tänkas göra för att smyga förbi en detektor oupptäckt. Dessa modifieringar var av typen små ändringar av ordval, översättning av ord, och även små skrivfel ("typos"). Detta inspirerat av vad vi vet riktiga angripare gör: De parafraserar, injicerar felstavningar, eller kör texten genom en maskinöversättare för att undvika filter.

Resultaten? Ingen av detektorerna får 'A.' Både GLTR och DetectGPT hanterade parafrasering relativt bra, en deras "accuracy" föll dramatiskt för enkla felstavningar. Bara några enkla felstavningar reducerade DetectGPTs "recall" till 40%. ZeroGPT tappade koncepten helt. Den fångade i stort sett inte någon av de modifierade AI-genererade meddelandena.

Så den som vill undgå detektion har fortfarande flera enkla och verkningsfulla verktyg att ta till. Bara att strö lite felstavningar i texten så kommer man igenom. Det är ju på inget sätt en avancerad metod för att lura en detektor.

Så vad kan vi lära oss? Tja, allt är väl inte helt förlorat. Mot en naiv angripare så finns det ändå hopp att hitta, iaf de flesta, av de AI-genererade meddelandena utan att för den sakens skulle drunkna i falsklarm (som alltid så kommer högre träffsannolikhet med flera falsklarm som ett brev på posten). Men om angriparna bara gör några enkla försök att maskera sig så ser det genast värre ut. Då klarar sig detektorerna betydligt sämre.

Så, lita inte på en ensam detektor, och inte i det enskilda fallet. Man måste tyvärr, som så ofta, väga samman ledtrådar från flera källor, inklusive mänskliga sådana, och fatta ett beslut utan att kunna vara hundra procent säker på att det är rätt.

Och, som alltid, lita inte på vad det står i reklamen. För att veta hur produkter presterar så måste man testa själv. Om ni är intresserade av att läsa hela avhandlingen så maila mig så skall jag se till att den skickas när den är färdig.

P.S. Jag körde just ovanstående text i ZeroGPT med resultatet att den är skriven av en människa "0% skriven av AI GPT." Men är den det? Ja, det är ju den intressanta frågan...

4. DFRWS 2026 Linköping Sponsorship

DFRWS
DIGITAL FORENSICS RESEARCH CONFERENCE

EU-sponsorship@dfrws.org

EU SPONSORSHIP PROSPECTUS

BENEFITS	PLATINUM	GOLD	SILVER	BRONZE	STUDENT SCHOLARSHIP
Limited Sponsorships	1	3	4	10	∞
Logo on Website, Screen Graphics, and Printed Conference Materials	✔	✔	✔	✔	✔
Logo on Lanyard	✔	✘	✘	✘	✘
Ad in Program	Full Page	Half Page	Quarter Page	✘	✘
Exhibit Space	✔	✔	✔	During Demo Session only	✘
Tables provided	2x6ft Table	6ft Table	6ft Table	Cocktail Table	✘
Virtual Attendee Registrations	Up to 30 (€3,600 EURO value)	Up to 20 (€2,400 EURO value)	Up to 15 (€1,800 EURO value)	Up to 10 (€1,200 EURO value)	Up to 5 (€600 EURO value)
Full Conference Passes	4 (€3,380 EURO Value)	3 (€2,535 EURO Value)	2 (€1,690 EURO Value)	1 (€895 EURO Value)	1 (Student)
AMOUNT	€10,000 EURO	€6,000 EURO	€4,500 EURO	€2,500 EURO	€2,000 EURO

WHY BECOME A DFRWS SPONSOR?

Established in 2001
DFRWS is the longest running digital forensics research event in the world. Conference topics continue to lead & shape the field.

Global Reach & Visibility
With 3 annual conferences on different continents, DFRWS events are an excellent venue to showcase your products and services, attracting new customers on a global level.

Access the Leaders and Decision Makers
Our attendees are the leaders and decision makers within their organizations.

Dedicated Following
Find experienced, vetted talent and develop stronger relationships within a broad community.

Non-Profit, Volunteer-Driven, Multi-Disciplinary
DFRWS brings digital forensics community leaders from Academia, Government, Law Enforcement and Industry together.

LEARN MORE at **dfrws.org**

5. Årets sista nätverksträff

26 november Kl.9:30–16:30
MSAB:s kontor i Stockholm

Tema: **Attacker mot samhällets infrastrukturer**

Dagen innebär också att vi får stifta närmare bekantskap med **MSAB**:s verksamhet.

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

Preliminär agenda (kommer att uppdateras)

09:30 — Registrering och kaffe

10:00 — Välkomna till MSAB, Martin Westman, Exploit Research Manager

10:10 — På gång inom DFS, Niclas Fock, Lena Klasén

10:30–12:00 — Keynote Talks
- Keynote I :Bacteria Don't Lie: Harnessing the Microbiome for Forensic Intelligence Eran Elhaik, Lund University (45 min)
- Keynote II : Investigative Readiness: Bridging Cyber Incidents and Criminal Investigations Odin Heitmann, Kripos, Norge (45 min)

12:00–13:15 — Lunch inklusive visning MSAB

13:15–16:00 — Keynote Talks och företagspresentation
- Företagspresentation — DataExpert, Rasmus Andersen, Managing Director (30 min)
- Keynote III : Advanced unmanned aerial helicopter systems for dual-use, Mikael Taveniku Evolved Systems Scandinavia AB (45 min)
- Keynote IV — Acid rain, Professor Anders Carlsson, BTH (45 min)
- Keynote IV Polisens drönarverksamhet, Johan Dahlén, Polisregion Syd

16:00 — DFRWS 2026 i Linköping 23–27 mars (kort info)

16:15 — Avslut. (Kaffe serveras under eftermiddagen)

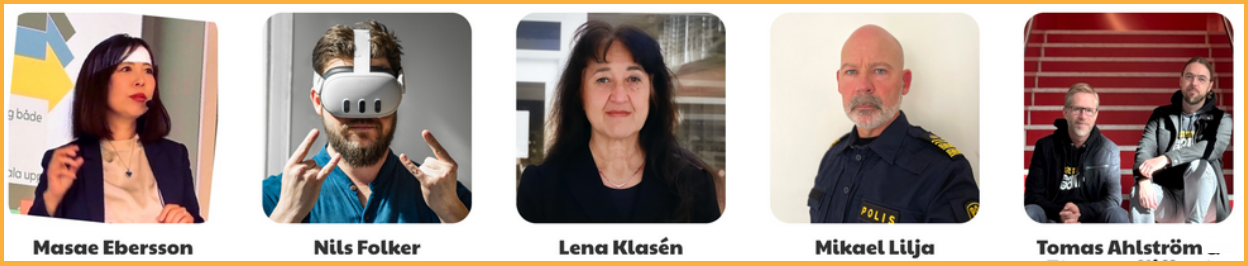
DIGITAL FORENSICS SWEDEN

6. GAMES FOR CHANGE

Vårt projekt, **Interaktiva Digitalla Tvillingar genom Multimodal AI** ska presenteras vid **East Sweden Game Summit** kl.16:00 den 20e november i Ebbepark, Linköping

This session explores how game technology can strengthen public safety, security, and forensic work — with short talks on visionary projects, data visualization tools, and real needs from law enforcement and industry.

On stage:
Masae Ebersson, Santa Anna IT Research Institute AB/ AI Sweden
Nils Folker, Lutra Interactive AB
Lena Klasén, Swedish Police /Linköping University
Mikael Lilja, Swedish Police
Tomas Ahlström, East Sweden Game



7. Flera länkar

- **DFRWS EU konferens 2026** i Linköping: https://dfrws.org/
- Digital Forensics Sweden, vår egen site: https://www.digital-forensics.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!