DIGITAL FORENSICS SWEDEN

digital-forensics.se

Innehåll

Lägg till i din kalender

- Nätverksträff: **den 28e maj** kl. 10.00 -14.00 i Linköping

- Den årliga EU-forskning konferensen **DFRWS 2026** kommer att hållas i Linköping **den 23e – 27e mars 2026.**

Se sidan 3 för mer info.

1. Inledning

Välkomna till årets första nyhetsbrev från Digital Forensics Sweden!

2024 blev ett år fullt av aktivitet och framgångar för Digital Forensics Sweden (DFS).

Vi har för första gången sammanställt en enkel årsrapport (bifogas detta nyhetsbrev) där vi kort redogör för saker som hänt och gjorts under det gångna året. Det vi saknar är partnerperspektivet, så under det här året vill vi få veta mer om vad som händer hos er alla, som relaterar till DFS och det nätverk och ekosystem vi tillsammans utgör.
En bra början är att skriva till oss och berätta vad som pågår, så tar vi gärna med det i våra nyhetsbrev.

Under året kommer vi att fortsatt arbeta för finansiering av en nationell forskningsmiljö, baserat på att det i forskningsproppen finns öppningar för medel avsatt till ”praktiknära professionsforskning inom brottsbekämpning”.

Med nyhetsbrevet denna gång följer också en placeholder för nästa års digitalforensiska konferens, DFRWS2026, som för första gången kommer att äga rum i Sverige, närmare bestämt på Linköpings Universitet och vill förstås se så många av er som möjligt här på plats, den 23-27 mars 2026.

Ni har väl noterat att nätverksträffen den 21/3 blir exceptionellt spännande med både Europol som pratar europeiska språkmodellprojekt, och AI Sweden som berättar om hur man arbetar med läckande AI-modeller för att säkerställa att träningsdata in ta kan återskapas.

Till sommaren planerar vi för en nätverksträff med fokus på Utbildning inom Digital Forensik, och efter sommaren blir det cyber crimes och fokus på kritiska samhällsinfrastrukturer.
Vi välkomnar flera nya partners i nätverket, och vi vill gärna erbjuda er som är nya en möjlighet att presentera er på kommande nätverksträffar under året.

Nyhetsbrevet bjuder som vanligt på en krönika av Professor Stefan Axelsson, liksom lite information, tips och tankar från våra två doktorander, Johnny Bengtsson och Johannes Olegård.

Önskar er som alltid trevlig läsning!
Niclas Fock

2. DFRWS 2026 kommer att hållas i Linköping

Vi är glada att meddela att vi har blivit valda som värdorganisation tillsammans med LiU, för konferensen "DFRWS2026" https://dfrws.org , som kommer att hållas i Linköping!

Konferensen äger rum den 24–27 mars 2026, med en fördag för nätverkande mellan partnerorganisationer den 23 mars.

3. Senaste nyheterna inom AI i forensik

AI för rättsmedicin: Förutsäger hjärnskador med hög precision

Forskare vid Oxford har utvecklat en AI-modell som kan förutsäga traumatiska hjärnskador (TBI) baserat på polisrapporter och biomekaniska simuleringar. Modellen uppnår 94 % noggrannhet för skallfrakturer och kan hjälpa polisen att bättre bedöma skador vid brottsutredningar. Studien publicerades i Communications Engineering.

Läs mer här: University of Oxford

Ett relevant forskningprojekt vid Linköpings universitet

"Advanced Digital Forensics Research with Focus on Deep Learning"
Principal Investigator: Shizhen Chang (jan 2025 - jan 2026)

Projektet fokuserar på att utveckla avancerade AI-modeller för att upptäcka bildmanipulationer, analysera kriminella aktiviteter och återställa skadade bilder.

För mer information: supr.naiss.se

Australiska federala polisen: “Vi har inget val än att använda AI”

Enligt den australiska federala polisen (AFP), utredningar som genomförs av omfattar i genomsnitt 40 terabyte data, inklusive material från 58 000 ärenden om barnexploatering årligen. Ett cyberintrång rapporteras var sjätte minut.

"Vi har inget val än att använda AI"

AFP deltar i statens Copilot AI-test och utvecklar egen AI med Microsofts verktyg, inklusive översättning av sex miljoner e-postmeddelanden på spanska och analys av 7 000 timmars videomaterial.

"Att en människa granskar 7 000 timmar är omöjligt – AI spelar en avgörande roll,”

Läs mer här: The Guardian

4. Forskningsnytt #1

Johannes Olegård

Min forskning på frågan "Vad ska man logga egentligen?" fortsätter. När man bygger IT-system så vill man se till att systemet skapar loggfiler och att dessa filer beskriver händelseförlopp tillräckligt bra för att man ska kunna dra bra slutsatser under forensisk utredningar (t.ex. efter att systemet blivit hackat). Det finns förvånansvärt lite forskning på vad man man ska logga och hur mycket som är "tillräckligt" (för det går ju alltid att logga *mer*).

Jag fick nyligen en artikel [1] accepterad till DFRWS EU [2], vilket är en av de större och finare forskningskonferenserna i området. Efter konferensen publiceras artiklarna i den öppna tidskriften "Forensic Science International: Digital Investigation" [3]---så jag kan tyvärr inte länka direkt till artikeln än. Artikeln handlar om att spara "kausalitetsinformation" i loggfiler. Om två olika program i samma IT-system har pratat med varandra, så är man oftast (i en forensisk utredning) intresserad av att "korrelera" loggar från de två programmen, dvs. lista ut vilka rader i ena loggen hänger ihop med vilka rader i andra loggen. I dagsläget är det en kvalificerad gissningslek som bygger framförallt på tidsstämplar. I min artikel påpekar jag att man faktiskt kan designa sitt IT-system så att man slipper gissa, dvs. att man kan spara kausalitetsinformation i loggarna från början (i form av referenser till "event IDn")---vilket gör korrelation mycket lättare. I den här första artikeln så gör jag en liten proof-of-concept.

Engelska sammanfattningen från artikeln:
It is generally agreed that logs are necessary for understanding cyberattacks post-incident. However, little is known about what specific information logs should contain to be forensically helpful. This uncertainty, combined with the fact that conventional logs are often not designed with security in mind, often results in logs with too much or too little information. Events in one log are also often challenging to correlate with events in other logs. Most previous research has focused on preserving, filtering, and interpreting logs, rather than addressing what should be logged in the first place. This paper explores logging sufficiency through the lens of Digital Forensic Readiness, and highlights the absence of causal information in conventional logs. To address this gap, we propose a novel logging system leveraging ``gretel numbers'' to track causal information---such as attacker movement---across multiple applications in a tamper-resistant manner. A prototype, implemented using the Extended Berkeley Packet Filter (EBPF) and an Nginx web server, shows that causality tracking imposes minimal resource overhead, though log size management remains critical for scalability.

Nästa artikel kommer förmodligen handla om hur man bygger in "anti-tampering" mekanismer i ett sånt här system med hjälp av (och för att skydda) kausalitetsinformation---dvs. att man gör det svårare för en hackare att ta bort eller förvränga information i loggar, eller åtminstone gör så att hackaren inte kan göra detta oupptäckt. Det funkar på lite samma sätt som man med bokföring (transaktionsloggar) kan upptäcka vissa typer av bedrägerier. Det finns redan liknande forskning på anti-tampering mekanismer [4], men den skyddar inte kausalitetsinformation.

På sikt är också tanken att försöka taxonomisera undersökningsfrågor i cyberincidenter. Om vi vet vilka undersökningsfrågor vi förmodligen kommer ställa i framtiden, så kan vi ta reda på vad för data som faktiskt hade behövts för ge bra svar på de frågorna---speciellt data som inte loggas i dagsläget.

Johannes

**Källhänvisningar finns på sista sidan under "Flera* länkar"

5. Forskningsnytt #2

Johnny Bengtsson

Metaartikel om en artikel

Förmodligen är det många av oss som har arbetsdagar som kan upplevas långa. Eller saknar progress. Så har det varit lite med skrivande på sistone. Jag sitter och formulerar och omformulerar. Ändrar lite, plockar bort någon mening. Fyller på med en ny mening. Den ser nästan likadan ut som den jag valde att ta bort. Den nygamla meningen känns något mer lättläst ut. Betyder den samma sak? Har jag definierat begreppen tydligt nog? Min kritiska självinsikt säger mig att jag näppeligen torde vara förstahandsvalet som artikelskribent på en nyhetsbyrå. Jag skulle åtminstone inte anställa mig själv för en sådan arbetsuppgift där snabba nyhetsartiklar måste ut.

Mitt fokus i skrivande stund är att få till en tillräckligt intressant och läsvärd introduktion till ett pågående manuskript som innefattar utforskande forskning i en driftsatt kontorsbyggnad [1, 2]. Förhoppningsvis ska det kunna leda till något som är publicerbart. För att tillföra fördjupade domänkunskaper till manuskriptet har jag tillfrågat Fredrik att vara medförfattare, vilket han har accepterat. Fredrik är konsult vid ett stort konsultbolag och disputerad inom området energioptimering av fastigheter. Han har, liksom många andra goda personer i min omgivning, genomgående stöttat mig. I det här fallet har det bland annat handlat om utläsning av sensordata från de försök jag har genomfört på Testbädd Ebbepark samt tålmodigt besvarat de del allra flesta frågor jag haft om det specifika fastighetsautomationssystemet.

Publicerad artikel om tillförlitlighet i dataset

Det har även tidigare gått trögt med skrivandet, men togtack och lov fart fram mot senhösten förra året. Det akademiska skrivhantverket är det som har tagit allra mest tid att slipa på, något jag även skrev om i det förra nyhetsbrevet [3]. I slutet på förra året skickade jag in min första manuskriptversion till en referentgranskad tidskrift [4] som har ett gott renommé inom den it-forensiska forskningen. Valet av tidskrift i mitt fall väldigt enkelt. Dock ville jag försäkra mig om att den ändå fanns listad i Kanalregistret [5], vilket den var.

Kanalregistret, som för allmänheten kanske mer känd som norsklistan eller Norwegian List, syftar till att granska och lista akademiska tidskrifter utifrån ett antal kriterier som i slutändan avgör om det är en seriös vetenskaplig tidskrift. Det finns många tveksamma rovtidskrifter, eller predatory journals, som tar betalt för att publicera artiklar med tveksam akademisk verkshöjd.

Manuskriptet passerade den ansvarige chefredaktörens nålsöga och gick vidare för granskning. Referenterna hade gett mig ett berg av kommentarer och förbättringsförslag att bemöta. Skulle jag lägga mig på rygg och ge upp? Nä, jag valde att återkalla jul- och nyårsledigheten för att göra allt i min makt för att hinna med slutdatumet för bot och bättring. Slitet gav resultat, artikeln blev betydligt bättre i alla avseenden, men ökade samtidigt i omfattning med två sidor. Så i januari blev den slutligen publicerad [6].

Den publicerade artikeln syftar till att medvetandegöra att loggdata kan ha felaktigheter i sig, trots mekanismer för datakorrigering. Det sista påståendet om att systemet kan laga data skrev jag nog inte i artikeln, men borde åtminstone vara uppenbart för erfarna it-forensiker. Felaktigheter kan i sin tur leda till felaktigt dragna slutsatser. Visserligen har den här artikeln en särskild betoning på tillämpningsområdet hem- och fastighetsautomationssystem, men torde vara generellt gällande för fler it-system och tillämpningsområden.

För att ge stöd för mitt påstående om att inte godtroget lita på registrerade sensordata behövde jag komma på något som är konkret och lättbegripligt för utomstående. Likt min käre barndomsvän Professor Balthazar [7] vandrade jag mentalt fram och tillbaka och funderade, och funderade... Till sist landade jag i att försöka genomföra ett antal icke-invasiva, alltså ickeförstörande, angrepp mot koldioxid- och PIR-sensorerna installerats i det då outhyrda kontorsplan och som jag av det allmännyttiga fastighetsbolaget [8] fritt hade fått disponera.

Angreppen mot fastighetsautomationssystemet innebar att antingen gömma sig från sensorerna och därmed undgå händelseregistrering i loggsystemet eller att skapa falska sensoriska händelser, varpå falska aktiviteter ickeinvasivt frammanas och därmed nedtecknande av dessa i loggningen. Försöken genomfördes genom att på betald arbetstid leka Charles-Ingvar Jönsson, den erkänt skarpaste kniven i Jönssonligans bestickläda, och mannen vars hiss åtminstone till synes ser ut att gå ända upp, trots att alla hästar ännu inte är inräknade.

Koldioxidsensorer

Koldioxidsensorkurragömma var inget jag tidigare erfarit. Därför krävdes det ett nytt sätt att tänka. Till att börja med, så tog jag med mig en rulle soppåsar som var avsedda att fungera som ett slags luftbehållare. Trettio liter utandningsluft innebär inte särskilt mycket närvarotid. Men soppåsarna höll tätt. Sedermera köpte jag en rulle svarta sopsäckar för samma ändamål. Dessutom engagerade jag Fredrik och Sara i syfte att producera extra mycket koldioxid och som skulle andas ut i de tilldelade sopsäckarna. Dessvärre såg säckarna ut att läcka, vilket påverkade mätresultaten negativt. Koldioxidhalten ökade i rummen vi gjorde försök i.

Slutligen tänkte jag att en uppblåsbar badleksak kan vara lösningen på problemet. Tyvärr var det inte badsäsong, så därför fanns det inte någon svensk nätbutik som tillhandahöll uppblåsbara ananaser eller flamingos. Lösningen blev en friluftsbutik. Inte för att de erbjuder fri luft som namnet kan tyckas antyda, utan för att köpa mig en dyr luftmadrass. Sådana är som bekant utformad att hålla inblåst luft ofri. Med luftmadrassen ökades uthålligheten till över fyra minuter innan den var full. Det gick således väldigt bra att gömma sig från koldioxidsensorerna i respektive rum.

PIR-sensorer

En PIR-sensorer, eller egentligen pyroelektrisk infraröd sensor, reagerar på temperaturförändringar. PIR-sensorer används för att detektera närvaro, vilket ger stimuli till olika beslutsstöd såsom hem- och fastighetsautomationssystem, belysningssystem, inbrottslarm med mera.

En initial inspirationskälla för att överlista PIR-sensorerna var en artikel i Financial Times [9] som jag läste, men av en helt annan anledning. Artikeln beskriver i en händelse där ukrainska soldater alldeles i början av den nu pågående ryska invasionen lyckades att undgå de ryska drönarnas termiska kameror genom att hålla liggunderlag (ukr. karemats) över deras huvuden. Läsningen fick mig att dra på mungiporna. Kan denna erfarenhet från en helt annan verklighet användas i mitt forskningsprojekt?

Initialt köpte jag ett liggunderlag för att termiskt skyla mig från PIR-sensorerna. Visserligen gick det att med en termisk kamera bekräfta en avskärmad värmestrålning, men det var praktiskt omöjligt att hantera liggunderlaget med en hand, samtidigt som jag upplevde det praktiskt omöjligt att öppna och stänga dörrar. Gissningsvis är det skillnad mellan en termisk kamera med begränsad pixelupplösning och PIR-sensorer med relativt brett synfält och som är placerade på marknära höjd.

Jag har sedan tidigare klurat på varför metallfolietäckta engångsnödfiltar är så bra och landade då i att dessa borde vara fantastiska på att återreflektera den utstrålande kroppsvärmen. Här blev en annan friluftsbutik en räddning. Jag köpte alla nödfiltar de hade i butiken. Det kunde på plats konstateras att dessa faktiskt går att använda för att gömma sig från PIR-sensorerna, men även dessa svåra att hantera med en hand.

Det sista angreppet jag ville åstadkomma var att skapa falska spår i fastighetsautomationssystemet.
Detta skedde genom att jag fick låna min kollega Jimmy till att flyga drönare inne i det öppna kontorslandskapet.
Således skapades falska positiver i loggningssystem.

Detta kan skenbart misstolkas att en person sakta har promenerat inne i byggnaden, medan det i själva verket var en värmestrålande drönare som åstadkom spåren.

Avslutningsvis så skulle den här metaartikeln kunna bli mycket längre, men jag tror att jag nöjer mig för idag.

Johnny

Källhänvisningar

---
[1] Testbädd Ebbepark (2025). https://www.ebbepark.se/projektet/testbadd/. Läst 2025-03-14.
[2] Ebbepark (2021). Nu öppnar Spektrum i Ebbepark (2021). https://www.ebbepark.se/nyheter/nu-oppnar-spektrum-i-ebbepark/. Läst 2025-03-14.
[3] Bengtsson, J. (Ebersson, M., red. 2024). Nyhetsbrev #2/24 (4), Forskningsnytt #2. https://www.digital-forensics.se/category/nyhetsbrev/. Läst 2025-03-14.
[4] Geradts, Z. och Nikkel, B. (red. 2025). Forensic Science International: Digital Investigation. https://www.sciencedirect.com/journal/forensic-science-international-digital-investigation. Läst 2025-03-14.
[5] Kanalregistret (2025). https://kanalregister.hkdir.no/. Läst 2025-03-14.
[6] Bengtsson, J. (2025). The ghost in the building: Non-invasive spoofing and covert attacks on automated buildings. https://www.sciencedirect.com/science/article/pii/S2666281725000198. Open access.
[7] Wikipedia (red. 2024-11-20). Professor Balthazar. https://sv.wikipedia.org/wiki/Professor_Balthazar. Läst 2025-03-14.
[8] Sankt Kors Fastighets AB (2025). https://sanktkors.se/. Läst 2025-03-14.
[9] Judah, T. (2022). How Kyiv was saved by Ukrainian ingenuity as well as Russian blunders. https://www.ft.com/content/e87fdc60-0d5e-4d39-93c6-7cfd22f770e8. Läst 2025-03-16.

6. Forskningsnytt #3

Johnny Bengtsson

Elda på bara, så löser vi det digitala!

Genom åren på NFC och i den tidigare myndigheten Statens kriminaltekniska laboratorium (SKL) har jag fått möjligheten att beträda en mängd platser som är otillgängliga för de allra flesta. Men inte någon brandplats. I denna kontext syftar en brandplats exempelvis på byggnader som har utsatts för en brand och där det finns ett intresse av att utröna misstanke om begånget brott.

I min förra text [1] avslutade jag med att det kanske blir någonting skrivet om brandplatsundersökningar och hur it- och IoT-forensik kan tillföra kompletterande information till sådana undersökningar.
I samma text refererades det till det rikligt detaljerade poddavsnitt 3 i Aftonbladet-podden "Djävulen finns i detaljerna" [2].

Det avsnittet handlar om en spektakulär mordbrand. Ärendet involverade bland annat två olika fjärrströmbrytare, kvitton, en lödkolv, en robotdammsugare och en surfplatta. Utan att gå in på detaljer i den här texten, så har erfarenheterna från detta ärendet fört mig in på tankarna kring kombinationen brandutredningar och it-forensik. Att ärendet i slutändan kunde uppklaras och leda till fällande dom tror jag till stora delar berodde av det goda samarbetet mellan berörd personal vid NFC och polisens brandutredare.

Med brandutredare inom polisen menas vanligen erfarna kriminaltekniker som har genomgått en särskild påbyggnadsutbildning. En av NFC:s många åtaganden är att utbilda kriminaltekniker och brandutredare. Under hösten 2024 genomfördes kursen "Platsundersökning brand - fördjupning", ett sex veckor långt myndighetsinternt brandutbildningsprogram fördelat på tre tvåveckorskursblock.

En nyhet med denna utbildningsomgång var att en heldag avsattes till it-forensik. I samband med detta fick jag frågan och förtroendet att planera och genomföra detta utbildningsmoment tillsammans med två kursansvariga forensiska experter inom brandutredning. Det som jag till stora delar valde att ta upp var hur traditionell it-forensik både generellt och specifikt skulle kunna tillämpas på brandplatser, såsom privatbostäder, kontor och offentliga byggnader och fordon. Det sistnämnda är också intressant för en brandutredare, då det emellanåt förekommer anlagda bilbränder, men även att en del elfordon är försedda med videokameror som kan tänkas ha spelat in händelser som skett i samband med ett brandförlopp. Personligen kan jag inget om vare sig brandutredningar eller vilka förmågor som krävs för detta. Mina undervisningskollegor kan förmodligen det mesta om brandutredningar, men kanske brister i kunskaper om komplex it-forensik. Detsamma kan säkert sägas om den genomsnittlige kursdeltagaren. Vi valde upplägget att köra presentationer med högt i tak och gott om utrymme för diskussioner, vilket även hjälpte mig att bli varse om tänkbara kunskapsbehov som framledes kan behöva att tillgodoses.

Förslag på framtida arbeten i gränslandet brand och it-forensik

---

Hur går det då att resonera kring framtida arbeten beträffande brandplatsundersökningar och it-forensik? Parallellt med andra tankar som upptagit delar av min vakna tid, så har den it-forensiska brandplatstänkarmössan för stunden resulterat i följande:

Förutom traditionella spår kan brandplatsundersökningar också innefatta konfigurations-, användar - och aktivitetsdata från elektroniska styr- och övervakningssystem och konsumentelektronik. Data kan under vissa omständigheter extraheras, trots exponering av höga temperaturer, chock, väta, elektromagnetisk strålning eller konduktiva sotpartiklar. Exempel på detta har en forskargrupp vid Université de Lausanne (UNIL) praktiskt påvisat, där lyckad datautläsning och analys har gjorts av ett hemautomationssystem som utsatts för en anlagd men kontrollerad brand [3].

Utlästa data kan utgöra loggade systemhändelser som skett parallellt med brandförloppet. Dragna slutsatser kan potentiellt användas för att beskriva aktiviteter som både har föregåtts av branden, händelser under eller efter brandförloppet. Några exempel på produkter som loggar händelsedata är nyare vitvaror som tvättmaskiner, diskmaskiner och kylskåp, smartteveapparater, uppkopplade badrumsvågar, robotdammsugare, övervakningssystem, brandlarmsystem samt hem- och fastighetsautomationssystem för styrning och övervakning av inomhusmiljön.

Den andra kategorin är elektroniska produkter med kroppsmätande sensorer som vi bär på oss eller med oss; vanligen IoT-produkter som kräver datautbyte med en extern funktion eller tjänst. Produktsegmentet kallas vanligen wearables, smart wearables, wearable devices, wearable technology och liknande. Exempel på sådana IoT-produkter är smartklockor, aktivitetsarmband, smartringar och andra typer av kroppsmätande sensorer samt framtida smarta plagg med inbäddade sensorer.

Data från wearables exempelvis kroppssensorer ger annan typ av sidoinformation; tidsstämplade artefakter, såsom geolokalisering, biometriska data som pulsslag och syresättning och som kan beskriva aktiviteter och hälsotillstånd. Till kategorin wearables kan eventuellt även exempelvis även smartglasögon och andra liknande produkter höra; gjorda ljud- och videoinspelningar av sådana kan ge värdefulla vittnesuppgifter av individer som vistats på eller i närheten av brandplatsen.

Mot bakgrund av de många elbränder relaterat laddning av batterier med hög energitäthet, som exempelvis branden i ett flerfamiljshus i Norrköping under 2023 och där 150 personer fick evakueras [4, 5], så har jag funderat över en tredje kategori informationsbärare: utrustning relaterade batterier, batteriladdare och energilagringssystem. Idag finns det ett allmänt koncept för batteriövervakning: battery management system (BMS). I korthet inbegriper BMS-funktionaliteten batteriövervakning av exempelvis spänningar och strömmar, temperaturer och laddningsnivå, eller state-of-charge (SOC), algoritmisk cellbalansering, temperaturhantering och förebyggande skydd mot överladdning [6..9]. Utan att ha påbörjat eget utforskande av BMS:er, så kan det ändå kan vara värt att någon i framtiden studera dess möjligheter och begränsningar samt tillämpbarheten beträffande it-forensik. Denna 'någon' innebär nödvändigtvis inte jag. En sak till: det blir naturligtvis en smärre it-forensisk utmaning om själva BMS-kretsen har brunnit upp eller tagit skada av en batteriexplosion.

Andra aspekter som kan tänkas höra till den här kategorin är kvalificerade batteriladdare; exempelvis laddboxar avsedda för elfordon och laddare för batterilager avsedda för mellanlagring av producerad solel. Även här siar jag lite och gissar på att det kan finnas tidstämplade data av intresse. En aspekt är att om laddutrusningarna är internetanslutna, så kan data ha lagrats på servrar som står på annan plats än på själva brandplatsen.

I sammanhanget ser jag det värdefullt att utröna om det finns sparad loggdata i exempelvis energilagringslösningar med egna battericeller, till exempel UPS:er (av uninterruptible power supply) som fungerar som ett extrabatteri som träder in vid spänningsbortfall i elnätet, power station-enheter, kraftfulla batterier som levererar 230 V växelspänning och avsedda att fungera på liknande sätt som en powerbank, elektroniska system för automatiserad styrning och övervakning av mellanlagring av producerad el i solcellssystem eller elanslutna elfordon i kontexten av framtida implementationer inom ramen för V2X-protokollet. Det är således både ur brandutredande och it-forensiskt hänseende är intressant att det framöver kikas närmare på det övergripande V2X-protokollet med underliggande tillämpningsområden, såsom V2H (vehicle-to-home), V2G (vehicle-to-grid) och V2V (vehicle-to-vehicle).

Slutligen, det förefaller inte helt otänkbart att vissa typer av batteripack med ett stort antal litiumjonceller avsedda för exempelvis elcyklar och elsparkcyklar också kan ha internt sparad information som kan vara relevant för brandutredningar. Men även här krävs det nog att laddelektroniken är relativt intakt.

När brandutredningar och it-forensik är som ler och långhalm

Jag tänker åtminstone fyra olika scenarion där it-forensik kan vara intressant att undersöka som stöd till en brandutredning: 1) den datalagrande elektronikkonstruktionen, eller hårdvaran, är den enskilda orsaken till branden, 2) hårdvaran orsakade branden tillsammans med andra och icke-elektroniska komponenter, 3) hårdvara fanns närvarande på brandplatsen, men var inte del av själva brandförloppet samt 4) hårdvara som användes av vittnen eller andra personer i brandens närhet.

För att illustrera med några fiktiva och verkliga exempel: 1) en hårdvaruenhet programmeras för att orsaka ett elfel som leder till värmealstring och som i sin tur startar en brand, 2) ärendet som beskrivs i [2] faller under den här kategorin, 3) en anlagd brand, vars händelseförlopp skulle kunna registeraras i likhet med [3], och 4) med stöd av exempelvis tidstämplade videoinspelningar och stillbilder kan det totala händelseförloppet lättare fastställas. Detta gäller särskilt om byggnaden är övertänd och bevismaterialen brinner upp.

Ett färskt exempel är skolskjutningen som inträffade i februari 2025 på Campus Risbergska i Örebro, där tusentals timmar video från allmänheten ligger till grund för kartläggningen av händelseförloppet [10, 11].

EAFS 2025

Tankarna och resonemanget från min sida är ännu i sin linda. Det som emellertid gläder mig är att jag har två abstrakt accepterade till konferensen European Academy of Forensic Science (EAFS 2025, https://eafs2025.org/) som går av stapeln mellan den 25-30 maj 2025 i Dublin.

Det ena abstraktet är för en muntlig presentation som rör 3D-utskrivna vapen och vapendelar [12], se förra nyhetsbrevet [1]. Det andra abstraktet är en posterpresentation [13] som just handlar om olika it-forensiska aspekter vid en brandplatsundersökning. Här har jag fått med mig några likasinnade seniora praktiker och prakademiker i Fredric (NFC), Olivier (UNIL) och Thomas (UNIL). Just det, en prakademiker (eng. pracademic) är ett väldigt användbart teleskopord myntat av Paul L. Posner [14]. En kortfattad innebörd är en person med praktiska erfarenheter som kliver in i akademin, eller vice versa [15].

Ses vi i Dublin i slutet av maj?

Johnny

Källhänvisningar

---

[1] Bengtsson, J. (Ebersson, M., red. 2024). Nyhetsbrev #2/24 (4), Forskningsnytt #1. https://www.digital-forensics.se/category/nyhetsbrev/. Läst 2025-03-14.
[2] von Wright, E. (2021). Avsnitt 3. Detaljerna som avslöjade mordbranden. https://www.aftonbladet.se/podcasts/ab/program/1363. Läst 2025-03-11.
[3] Servida, F., Fischer, M., Delémont, O. och Souvignet, T. R. (2023). Ok Google, Start a Fire. IoT devices as witnesses and actors in fire investigations. https://www.sciencedirect.com/science/article/pii/S037907382300124X. Läst 2025-03-16.
[4] Brantemo, A., SVT (2023). Fängelsestraff efter storbrand i Norrköping – knarkförsäljning avslöjades. ttps://www.svt.se/nyheter/lokalt/ost/fangelsestraff-efter-storbrand-knarkforsaljning-avslojades. Läst 2025-03-11.
5] Dahlström, S. (2024). Olycksutredning gällande brand Luntgatan i Norrköpings kommun. https://rib.msb.se/Filer/pdf/30916.pdf. Läst 2025-03-11.
6] TDT-BMS (2023). Battery Management Systems vs. Charge Controllers: What's the Difference? https://www.tdtbms.com/news/battery-management-systems-vs-charge-controllers-whats-the-difference.html. Läst 2025-03-11.
[7] Synopsys (2024). What is a Battery Management System? https://www.synopsys.com/glossary/what-is-a-battery-management-system.html. Läst 2025-03-11.
[8] Shidling, C. (2024). Safety Standards For Battery Management (BMS) In Electric Vehicle. https://cselectricalandelectronics.com/safety-standards-for-battery-management-bms-in-electric-vehicle/?citationMarker=43dcd9a7-70db-4a1f-b0ae-981daa162054. Läst 2025-03-11.
[9] MathWorks (2019). How to Develop Battery Management Systems in Simulink. https://se.mathworks.com/videos/series/how-to-develop-battery-management-systems-in-simulink.html. Läst 2025-03-11.
[10] Polismyndigheten (2025). https://polisen.se/aktuellt/nyheter/bergslagen/2025/februari/sju-kvinnor-och-fyra-man-dog-i-skolskjutningen/. Läst 2025-03-11.
[11] Karlsson, E. och Bergholtz, K. (2025). Tusentals timmar video granskas av polisen efter masskjutningen. https://www.svt.se/nyheter/lokalt/orebro/tusentals-timmar-video-granskas-av-polisen-efter-masskjutningen. Läst 2025-03-11.
[12] Bengtsson, J. (2025). Multidisciplinary forensic process for examinations of 3D printed firearms. Muntlig presentation vid European Academy of Forensic Science (EAFS 2025), Dublin.
[13] Bengtsson, J., Jonsson, F., Delémont, O. och Souvignet, T. (2025). Digital forensics as a complement to fire scene investigations and reconstructions. Posterpresentation vid European Academy of Forensic Science (EAFS 2025), Dublin.
[14] Posner, P. L. (2009). The Pracademic: An Agenda for Re-Engaging Practitioners and Academics. https://doi.org/10.1111/j.1540-5850.2009.00921.x. Läst 2025-03-11.
[15] Wikipedia (red. 2024-12-13). Pracademic. https://en.wikipedia.org/wiki/Pracademic. Läst 2025-03-11.

Övrig läsning

BotoX. Xiaomi M365 compatible BMS. https://github.com/BotoX/xiaomi-m365-compatible-bms. Läst 2025-03-14.
Embien (2025). Battery Management System: A comprehensive guide to Automotive BMS ECU. https://www.embien.com/automotive-insights/automotive-bms-ecu-battery-management-system-for-evs. Läst 2025-03-14.
HKJ (2015). Test/Review of Charger SkyRC MC3000. https://budgetlightforum.com/t/test-review-of-charger-skyrc-mc3000/37135. Läst 2025-03-14.
Schimpe, M. (2023). Logging In-Operation Battery Data from Android Devices: A Possible Path to Sourcing Battery Operation Data. https://www.mdpi.com/2079-9292/12/14/3049. Läst 2025-03-14.
ScienceDirect (2025). Battery Management System. https://www.sciencedirect.com/topics/engineering/battery-management-system. Läst 2025-03-14.

7. Krönika

Stefan Axelsson

Det händer mycket i världen just nu med ett förnyat fokus på försvar, beredskap, geopolitik, och andra militära frågor. Så jag tänker gå mot strömmen och istället prata om kanske det mest civila man kan tänka sig, nämligen civilrätt och hur den påverkar företags möjligheter att investera i immateriella tillgångar, till exempel programkod.

Jag har nu en handfull gånger varit inkallad som expert i fall som handlar om en ganska vanlig företeelse: Den börjar med att någon startar ett företag som går bra. Företaget köps upp av någon större spelare som antingen inte faller grundarna på läppen, eller helt sonika bestämmer sig för att lägga ner verksamheten till förmån för andra, utländska, enheter.

De som startade företaget bestämmer sig i ett slag att starta en konkurrerande verksamhet som snabbt levererar en snarlik produkt. Man hävdar ändå med bestämdhet att man minsann har återutvecklat produkten på rekordtid (man är ju trots allt experterna inom området) och att produkten rakt inte innehåller någon kod, eller på annat sätt baseras på immaterialrättigheter (upphovsrätt eller företagshemligheter) som, enligt avtal, tillhör den förra arbetsgivaren.

Detta slutar i att den förfördelade parten övertygar rätten om att det finns tillräckliga bevis för att kronofogdemyndigheten skall göra en gryningsräd för att säkra bevis, och så sitter man där med resultatet och behöver bestämma sig om man skall stämma i rätten eller inte.

För det är nu som problemen börjar på riktigt. Man får nämligen inte tillgång till hela det beslagtagna materialet (fattas bara annat) utan rätten tänker dels i "dokument", vilket är lite svårt att översätta när det rör källkod och t ex loggar från versionshanteringssystem, och dels så är de bara de "dokument" som träffar på förhand godkända söktermer som man får se.

Som ni förstår så kan det bli ett ganska magert och slumpmässigt urval, där man oftast blir stående med till exempel namnen på filer, men inte innehållet, och liknande.

Dessutom så förstörs det insamlade materialet direkt efter urvalet är gjort. Man har alltså ingen möjlighet att gå tillbaka om man nu skulle lyckas övertyga rätten om att kopiering faktiskt skulle ha skett. Förr så fanns det i all fall lagrat, men för några år sedan så gjorde man en omtolkning av lagen så att det insamlade materialet behövde förstöras innan dom fallit.

Man reduceras således till att försöka bygga en så stark indiciekedja att domstolen anser att denna väger över och kräver av svarande att det faktiskt förklarar varför materialet uppvisar så stora likheter som det faktiskt gör.

Så långt har undertecknad aldrig lyckats komma. I den handfull fall jag varit inblandad (på båda sidor skall sägas) så har kärande aldrig lyckats visa tillräckligt övertygande att man faktiskt har bättre rätt till kod eller andra artefakter, och att svaranden faktiskt gjort sig skyldig till upphovsrättsintrång och brott mot företagshemligheten.

Bilden skapades med DALL·E 3.

I det senaste fallet så hade vi, som jag tycker, en förhållandevis stark position där vi såg många, många, tydliga tecken på att kopiering skett. Vi fann, som bara ett exempel ur en lång lista, ett kryptografiskt certifikat som var identiskt i båda kodbaserna.

Men rätten plockade isär vartenda indicie med motiveringen att det ensamt inte utgjorde bevis, och kvar blev inte ens sagans tummetott. I fallet med certifikatet så sade domstolen till exempel att det ju knappast ens faller under upphovsrätten överhuvudtaget eftersom det enkelt genereras helt automatiskt och det då (naturligtvis) inte spelar någon roll om det kopieras.

Det kan jag hålla med om. Men vi tog upp det som bevis på att kopiering skett, inte för att det i sig skulle utgöra något större värde. Om man haft rent mjöl i påsen så hade man naturligtvis genererat ett nytt certifikat istället för att enskilt kopiera det gamla, när man nu dessutom hävdade att man inte kopierat koden i samma del av källkodsträdet. Trots att filnamnen visade förbluffande överensstämmelse.

När vi går igenom forskningen så visar det sig att frågan om hur man skall avgöra om kod ser misstänkt lik ut för att den är kopierad eller uppkommit naturligt på grund av liknande krav, utbildning, etc. så verkar denna fråga inte vara särskilt noggrant studerad.
Det tycker jag är lite märkligt. Det som är gjort är mest inom området att hitta fuskande studenter som kopierat varandras laborationer. Det är inte riktigt samma problem som vi brottas med här.

Som Knuth sade för många år sedan om programmen som kördes vid hans universitet: 90 per cent are "short Fortran and wrong."

Vilket justerat fortfarande är sant för oss som lägger stor del av vår tid på utbildning av studenter. Men hör talar vi om stora kodbaser som utvecklats under lång tid av flera aktörer. Det är ett helt annat problem.

Till detta skall läggas att vi idag lever med stora språkmodeller (se där kom det lite AI med på ett hörn ändå) som säkert skulle kunna användas för att ”tvätta” kopierad kod så att den fortfarande levererar samma funktionalitet men är omskriven på ett sådant sätt att det blir ännu svårare, för att inte säga omöjligt, att bevisa att den är oärligt tillkommen.

Sammanfattningsvis så borde detta vara ett ganska allvarlig problem för den som vill investera i företag vars värde består till stor del av programkod eller motsvarande; särskilt i de jurisdiktioner där det är svårare med "non compete"-klausuler i anställningsavtal, eller där dessa inte ger fullt skydd.

Men som forskare så blir man ju också lite uppiggad av dylika misslyckanden, eftersom det ger tillfälle att forska och lära sig mer! Så om någon är intresserad av att söka medel för forskning inom det här området så hör gärna av er.

Vi har redan bildat en liten preliminär grupp med mig själv och en av landets främsta professorer i software engineering samt några till som är intresserade av att dyka djupare, både tekniskt och juridiskt, i den här frågan.

Stefan Axelsson, 2025-03-13

8. Nästa Nätverksträff

Nästa nätverksträff
Preliminärt program:
Den 28/5 kl. 10.00 -14.00 i Linköping

Tema: träning och utbildning
Besök på nya Cyber Rangen på Linköpings Universitet

9. Flera länkar

[1] J. Olegård, S. Axelsson, Y. Li, When is logging sufficient? — tracking event causality for improved forensic analysis and correlation, Forensic Science International: Digital Investigation 52 (2025) [to appear in], DFRWS EU 2025 - Selected Papers from the 12th Annual Digital Forensics Research Conference Europe.

[2] https://dfrws.org/conferences/dfrws-eu-2025/

[3] https://www.sciencedirect.com/journal/forensic-science-international-digital-investigation/issues

[4] https://doi.org/10.1145/1323293.1294279

DFRWS: https://dfrws.org/

Digital Forensics Sweden, vår egen site: https://www.digital-forensics.se

the Nordic state of AI report by AMD/Silo AI
https://aifinland.fi/wp-content/uploads/2025/03/Silo_NSOAI4_WEB_2.pdf

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 Niclas Fock (niclas.fock@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!