Digital kriminalteknik och dess inverkan på integriteten av digitala bevismaterial

Pekka Ranta-aho

Kandidatavhandling i datavetenskap

Handledare: Marina Waldén

Fakulteten för naturvetenskaper och teknik
Åbo Akademi

Våren 2021

Ämne: Datavetenskap
Författare: Pekka Ranta-aho
Arbetets titel: Digital kriminalteknik och dess inverkan på integriteten av digitala bevismaterial
Handledare: Marina Waldén
Abstrakt: Denna avhandlings mål är att systematiskt gå igenom de olika stegen inom digital kriminalteknik då ett brottsfall utreds. Inledningsvis klargörs vilka krav som ställs på ett bevismaterial som kan presenteras i en rättegång i Finland, detta för att kunna ställa metodologin i rätt kontext. I metodologidelen går avhandlingen igenom i en kronologisk ordning de stegen litteraturen tar upp, börjandes med identifiering och dokumentering av digitala bevismaterial. I denna del behandlas exempel på typiska bevismaterial samt exempel på lite mer udda bevismaterial som kan stötas på i en brottsutredning. Avhandlingen går sedan in på tillvaratagning och beslagtagning av bevismaterial och hur detta bör ske på korrekt vis med målet att säkerställa att proceduren inte alternerar beviset. Följande delområde inom metodologin handlar om processering av digitala bevismaterial för att få tillgång och samla in data. Här tar avhandlingen upp olika risker förknippat med ämnet och vad litteraturen föreslår som bästa praxis. Här tas även upp som ett litet sidospår hur olika bias kan inverka på substansen av analysen och hur dessa fallgropar kan undvikas. Starkt kopplat till detta delområde hör analysdelen. Målet med analysdelen är att ge en bild av vad ingår i analysen och den vetenskapliga processen som bör följas för en effektiv och genomskinlig analys. Avslutningsvis behandlas rapporteringen av digitala fynd, vilken knyter ihop alla skeden till en helhet. I detta kapitel framhävs vad som är viktigt att tänka på då en rapport framställs och hur olika fallgropar kan undvikas. Avslutningsvis analyseras i avhandlingens diskussionsdel huruvida kraven för bevismaterialens integritet uppfylls varefter avhandlingen avslutas med ett

sammandrag och slutsatser avhandlingen kommit fram till på basis av litteraturen samt förslag på fortsatt forskning.	
Nyckelord: Digital kriminalteknik, metodologi, bevis	
Datum: 27.3.2021	Sidoantal: 21

Innehållsförteckning

1. Inledning

1.1 Problemformulering och syfte

Under senare år har behovet av digital kriminalteknik växt i takt med att samhället numera använder sig alltmer av digital kommunikation och digitala verktyg. Detta innebär att det finns ett behov av kunskap att hantera och analysera digitalt bevismaterial så att dess integritet inte blir satt på spel [1, s. 4]. I litteraturen läggs tyngdpunkten på just dessa aspekter. Ifall bevismaterialet och hanteringen av den kan ifrågasättas, betyder det att hela rättsprocessen kan ifrågasättas. I grund och botten handlar det om att värna om människors rättsskydd.

Syftet med denna avhandling är att göra en litteraturöversikt över vad som finns skrivet om digital kriminalteknik, dels för att möjligtvis kunna upptäcka möjliga luckor i metodologin, dels för att det är ett ämne som på universitetsnivå behandlats ganska liten utsträckning i Finland. Utifrån dessa frågor ställs avhandlingens grundfråga: uppfyller metodologin de integritetskrav rättsprocessen kräver?

Metodologin som framlagts finns till för att utövare av digital kriminalteknik ska kunna hålla sig till vissa allmänriktiga riktlinjer. Då en kriminalteknisk undersökning håller sig fast vid dessa riktlinjer minskar risken för misshantering av bevismaterial samt subjektiva tolkningar av bevismaterial. En stor del av metodiken har framställts av de som utövar digitalt kriminaltekniskt arbete [1, s. 4], vilket då leder till frågan hur tillförlitlig metodiken egentligen är? Denna har för avsikt att ge läsaren en överblick över grundpelarna i metodologin så att läsaren själv ska kunna göra en bedömning, dessutom presenteras skribentens egna tankar i slutet av avhandlingen.

1.2 Avgränsningar

Den digitala kriminaltekniken kan grovt delas in i två större delområden: kriminalteknik som berör nätverk och kriminalteknik som berör statiska apparater (hårdskivor, CD-ROM, USB-minnen etc.). Med kriminalteknisk undersökning inom nätverk syftar denna avhandling på företagsservrar eller infrastruktur som blir utsatta för cyberattacker och utredning av dessa. Denna avhandling kommer inte att behandla detta område, utan håller sig till digitalkriminal tekniskt arbete som berör statiska apparater och mestadels statiska data.

2. Krav på digitala bevismaterial (Krav på bevisföring? / Bevisföring inom rätten)

Lagstiftarens definition på digital utrustning hittas bland annat i tvångsmedelslagen kap 8 §20. Här avses digitalutrustning falla inom följande kategorier: datorer, teleterminalutrustning eller motsvarande tekniska anordningar eller informationssystem. Tvångsmedelslagen kap 8 §24 betonar även betydelsen i att bibehålla data som kan tänkas användas som bevisföring i dess ursprungliga form. Ytterligare kan nämnas Europeiska kommissionens definition [2] på digitalt bevismaterial som listar upp olika format av digital lagring av dokument i form av t.ex. e-post, textmeddelanden, fotografier, videon med mera.

Bevis som presenteras i en rättegång är alltid föremål för bevisprövning. Detta innebär att domstolen avgör ifall bevisvärdet uppfyller kraven för att det kan kunna tas i beaktande i ett domstolsbeslut [3]. Rättegångsbalken kap 17 §1 mom. 2 uttrycker detta på följande vis: ” *Domstolen ska efter att ha prövat de framlagda bevisen och andra omständigheter som har kommit fram vid handläggningen av målet avgöra vad som har bevisats eller inte bevisats i målet. Domstolen ska grundligt och opartiskt bedöma bevisvärdet av bevisen och de övriga omständigheterna genom fri bevisvärdering, om inte något annat föreskrivs i lag*.”. Detta innebär är domstolen har en s.k. fri

bevisvärdering vilket ger domstolen makt att göra en självständig bedömning av allt bevismaterial som läggs fram i en rättegång. Det här leder i sin tur till att domstolen är tvungen att motivera och begrunda varje enskilt bevis som läggs fram under en rättegång [4, s. 1247]. Det problematiska är för att fastställa med vilka metoder domstolen kan avgöra trovärdigheten på enskilda bevis och att beviset de facto berättar att någon händelse har inträffat [5, s. 20-21]. Ifall motparten bestrider det bevis som lagts fram är domstolen även förpliktigad att motivera varför den alternativa händelsen inte är trovärdig. Allt detta stiftas från grundlagen 2 kap §21 om medborgarnas rättsskydd, närmare bestämt att varje medborgare skall ha rätten till en rättvis och opartisk rättegång, rätten att bli hörd i sak samt rätten att få motiverade beslut [4, s. 1247].

Digital kriminalteknik är en vetenskap som är till för att lösa något juridiskt problem. Metodologin inom den digital kriminaltekniken är därför uppbyggd på ett sådant sätt att bevisen som läggs fram ska kunna tåla en kritisk granskning och resultaten av en undersökning ska även kunna reproduceras. Kort sagt baseras den digitala kriminaltekniken på den vetenskapliga metoden. Det viktigaste kravet som ställs på digitala bevismaterial är trots allt att ursprungsdata måste hållas oförändrade [6, s. 7-8, 10]. Detta innebär även att metoden som används för att ta tillvara data måste vara sådan att inga ändringar i data sker under beslagtagningen [6, s. 47]. Senare i avhandlingen behandlas tillfällen då dessa krav inte alltid uppnås och vad metodologin föreslår för att bevara bevismaterialets samt processens integritet. I kommande kapitel behandlar avhandlingen även andra viktiga metoder och principer som alla baserar sig på att uppehålla bevismaterialets trovärdighet.

3. Metodologin inom digital kriminalteknik

3.1 Allmänt om metodologin och kriminalteknik som vetenskap

Den digitala kriminaltekniken kan räknas till en ganska ung vetenskap som ännu inte helt och hållet hittat sin slutgiltiga form [7]. Jämförelsevis kan man titta på den klassiska formen av kriminalteknik vilken innebär brottsplatsundersökning efter bl.a. DNA-prov och fingeravtryck. Den klassiska formen av kriminalteknik har redan många år på nacken och många etablerade och allmänt godkända metoder. Exempelvis DNA-utlåtanden bestrids i dagens läge väldigt sällan och ses ofta som en slags ”Gold Standard” inom kriminaltekniken [6, s. 10]. För att belysa vilka utmaningar den digitala kriminaltekniken har som den traditionella saknar ges följande exempel: När det väl uppfunnits en metod på hur t.ex. ett DNA-prov skall tas och analyseras, går den samma metod att applicerat universellt på alla slags DNA-prov. Inom teknologin sker hela tiden nya innovationer i en sådan takt att det är svårt att hänga med och uppdatera samt definiera nya standarder och metodologier som innefattar den nya tekniken**.** För att klara sig i branschen krävs det en konstant uppdatering av den egna kunskapen [7].

Nuförtiden finns det ett flertal organisationer dedikerade till att upprätthålla en uppdaterad bästa praxis samt forskning inom området av digital kriminalteknik, som bl.a.: *European Union Agency for Law Enforcement Training* (CEPOL), *The European Union Agency for Network and Information Security* (ENISA), *The National Institute of Standards and Technology* (NIST) för att nämna några. Dessutom börjar det bli att vanligare att kriminaltekniska laboratorier ackrediteras av olika ackrediteringsorgan för att bevisa att de uppfyller vissa standard. Ackrediteringens huvudsyfte är att förbättra kvaliteten på arbetet i ett kriminaltekniskt laboratorium, göra upp standards som laboratoriets personal håller sig till, ha en utomstående part kritiskt granska laboratoriets verksamhet samt visa utåt att uppsatta standarder följs [6, s. 31, 43]. De olika standarderna som gäller inom digital kriminalteknik finns att hitta på *International Organization for Standardization* (ISO) sidor. Ytterligare cirkulerar

det ett flertal olika certifikat enskilda utövare av digital kriminalteknisk undersökning kan erhålla genom att gå olika kurser. Huvudmålet med en enhetlig metodologi är att samla in digitalt bevismaterial på ett sådant vis att det klarar en kritisk granskning samt står upp i en rättegång [8, s. 169].

3.2 Identifiering, säkerställande och dokumentering av digitala bevismaterial

Listan över potentiella digitala bevismaterial kan göras lång. Som tidigare nämnt i avhandlingen i kapitlet om bevis (kap 2), kan digitala anordningar listas upp på det vis lagstiftaren gjort i tvångsmedelslagen 8:24. På en mer detaljerad nivå kan uppräknas apparater som CD/DVD-skivor, USB-minnen, bärbara datorer, mobiltelefoner, modem m.m. Kort sagt så kan alla apparater kapabla till att lagra digital information potentiellt innehålla bevis. Trots att vissa föremål är mera självklara än andra lönar det sig att kolla en extra gång under uppsökning av bevismaterial under en utredning. Det förekommer t.ex. en mängd olika USB-minnesstickor som ser ut som leksaker och kanske det inte direkt faller in att en spelkonsol eller t.om. en bil kan innehålla en massa värdefull information [6, s. 48][9].

Då bevismaterialet identifierats gäller det att dokumentera och säkerställa detta [10, s. 13]. Hur beviset dokumenteras kan variera, men till bra praxis hör fotografering och egna anteckningar. Ytterligare kan sketcher på var bevismaterialet befann sig då det hittades vara till stor hjälp för uppklarning av omständigheter kring beviset i senare skeden [6, s. 47]. Syftet med dokumenteringen är alltså för att underlätta i ett senare skede, t.ex. under analysen, att gå tillbaka och se i vilket läget bevismaterialet befann sig då det togs i beslag. Detta kan ha stor inverkan på hur bevismaterialet bör tolkas. Dokumentering är det element som genomsyrar metodologins alla faser, med hjälp av utförlig dokumentering blir den kriminaltekniska processen lättare reproducerbar och bidrar även till undersökningens öppenhet och genomskinlighet [11, s. 7].

Säkerställandet av bevismaterialet innebär minimering av risken för ändringar i data eller rentav att data förstörs [12][10, s. 14-15]. I traditionell kriminalteknik innebär detta oftast att uppsättning av restriktioner på området som ska undersökas. Inom digital kriminalteknik är det inte alltid lika enkelt. En till synes obemannad dator som

är i gång kan vara uppkopplad till internet varifrån en utomstående person kan ha tillgång till datorn och dess innehåll, dessutom kan det ibland vara svårt att avgöra ifall en dator är igång eller inte. Risken att någon förstör eller alternerar data som kunde ha varit viktigt måste alltså tas i beaktande. Här ger metodologin inte heller några raka svar på vad som är det rätta tillvägagångssättet, men som bästa praxis anses ändå att koppla bort alla internetanslutningar samt koppla ur strömmen – speciellt ifall det konstaterats att data håller på att raderas [6, s. 48][11 s. 5][10, s. 14]. Ifall datorn kopplas bort från internet måste handlingen noggrant övervägas eftersom det medför en risk att tillgång till potentiella bevis som var fjärranslutna till datorn går förlorade.

Eftersom det inte alltid finns ett entydigt rätt svar på vad det rätta tillvägagångssättet är, så finns metodologin att falla tillbaka på, närmare bestämt dokumenteringen. Ifall alla åtgärder dokumenterats de samt omständigheterna kring dessa, är det lättare att i ett senare skede motivera sina beslut och då får även alla parter en överblick över potentiella data som gåtts miste om [6, s. 52-53].

Då bevismaterialet identifierats och säkerställts rekommenderas det även att granska potentiella manualer eller anteckningar som ligger i närheten. Dessa kan både hjälpa att förstå apparaten som skall undersökas bättre samt kan anteckningar innehålla viktig information så som lösenord och användaruppgifter. Dessa kan komma till hands speciellt vid analysering av krypterade data [6, s. 49][11, s. 5].

3.3 Tillvaratagande och hantering av digitala bevismaterial

Som tidigare nämnt kan metoden ett digitalt bevismaterial tillvaratas på inverka på den fortsatta utredningen av beviset. För att förtydliga vad som menas med detta tas följande exempel ur *John Sammons: The Basics of Digital Forensics*: Tänk dig att du stöter på en mobiltelefon som du identifierat som potentiellt bevis. Hur går du tillväga för att säkerställa beviset ifall mobiltelefon är igång och ansluten till internet? Här är vi tvungna att hålla metodologin i minnet, det vi gör får inte alternera data. En metod kunde vara att stänga av mobiltelefonen, men i och med att dagens smarta mobiltelefoner ofta är skyddade med lösenord riskerar vi att gå miste om potentiella

data på grund kryptering. Alternativt kan mobiltelefonen lämnas igång, men många mobiltelefoner har i dagens läge inbyggd funktionalitet som låter ägaren tömma innehållet i mobiltelefonen på distans ifall enheten är uppkopplad till internet [11, s. 4]. En bra kompromiss blir då att endera lägga mobiltelefon i flygplansläge eller ännu bättre i en s.k. *Faraday-påse* (en Faraday-påse hindrar yttre signaler från att nå mobiltelefonen). Tillgång till materialet i en krypterad mobiltelefon kan även riskeras ifall mobiltelefonens batteri laddas ur, vilket innebär att mobiltelefonen måste kopplas till en strömkälla. Exemplet ur Sammons bok åskådliggör hur alla skeden i tillvaratagandet av bevismaterial måste övervägas samt hur kryptering kan göra dessa beslut ännu svårare [6, s. 49-50].

Kryptering är något en digital kriminaltekniker måste hålla i tankar då bevismaterial tillvaratas. Kryptering kan tvinga en utredare att avvika från metodologins princip om att inte göra ändringar på data. Detta innebär med andra ord att bevismaterialet måste hanteras på ett sådant vis att det sker ändringar i data. Att operera på bevismaterial på detta vis refereras ofta till som *live digital kriminalteknisk undersökning* (eng. live digital forensics). Henry [13] listar upp viktiga steg en digital kriminaltekniker behöver ta vid en live digital kriminalteknisk undersökning. Det första och viktigaste steget är dokumenteringen. Efter dokumenteringen listar Henry upp digitala bevismaterial enligt volatilitetsordning:

1. CPU, cache & registerinnehåll
2. Kernel- och nätverksdata
3. Minne
4. Temporära filsystem (swap)
5. Data på hårdskivor
6. Molndata
7. Data som finns på yttre media (USB-minnesstickor, DVD, CD etc.)

Data i punkterna 1-4 är sådana som går förlorade då en dator stängs av [14, s.5]. Henry föreslår som nästa steg kopiering av datorns minne. Detta måste göras medan datorn ännu är igång och kräver körning av speciella program på datorn som är föremål för utredningen. Som resultat av att ett program laddas in i minnet och körs, alterneras både data i minne och data på hårdskivan. Därför är det viktigt att endast en person med kunskap inom området utför åtgärden samt att dokumenteringen innefattar vad

som gjorts och med vilka verktyg [6, s. 52]. Ifall det går att konstatera att datorns hårdskiva använder sig av kryptering, men att data för tillfället är okrypterade, kräver det dessutom att hårdskivan kopieras innan datorn stängs av. Här behöver en utredare också ha förståelse över vad som alterneras och potentiella data som uteblir [13]. Utöver detta måste den traditionella kriminaltekniken också beaktas så att ens handlingar inte förstör potentiella bevis som t.ex. fingeravtryck eller DNA [11, s. 5].

Bevismaterial som tagits i beslag bör lagras så att inga utomstående har tillgång till varken de fysiska eller digitala bevismaterialen. Till god praxis hör även att bokföra vilka personer som har behandlat bevismaterialet och när. Bevismaterial måste även säkerställas mot yttre katastrofer som bränder, vattenskador eller hårdvara som går sönder [6, s. 32-33, 53].

Som en röd tråd genom hela processen av tillvaratagande av digitalt bevismaterial hör dokumenteringen. En viktig sak som bör hållas i minnet under dokumentationen är att specificera vilka bevismaterial anteckningarna berör. Detta uppnås genom användning av serienumror eller andra unika identifierare [6, s. 52][10, s. 16].

3.4 Kopiering av digitala bevismaterial

Då ett bevismaterial samlats in är nästa steg att göra en kopia på bevismaterialets data. I metodologin kallas en sådan kopia för en kriminalteknisk kopia. Denna kriminaltekniska kopia (eng. forensic image) processeras sedan för vidare analys. Alltid är det inte möjligt att få en kriminalteknisk kopia av data ur en apparat, ibland får övriga alternativ duga [10, s. 14, 50]. I detta underkapitel redogör avhandlingen för vad en kriminalteknisk kopia på ett digitalt bevis innebär och hur integriteten på denna bekräftas.

En kriminalteknisk kopia av ett digitalt bevismaterial är en bitströmskopia av en bevismaterialet (t.ex. en hårdskiva). En bitströmskopia innebär att exakt varenda bit från hårdvaran kopieras (varje 0 och 1). För att uppnå detta mål krävs rätt programvara och teknisk utrustning som till exempel skrivskyddare. I de flesta fall kopieras bevismaterialet genom att hårdvaran som innehåller beviset kopplas till den tekniska

utredarens dator. Ifall hårdvaran kopplas rakt till den tekniska utredarens dator uppstår det en risk för datorn kan göra ändringar i hårdvaran, därför används skrivskyddare. Skrivskyddarens uppgift är att se till att data endast rör sig åt en riktning, vilket är från hårdvaran till kriminalteknikerns dator [10, s. 47].

Efter säkerställning av att inga nya data kan skrivas på bevismaterialet är nästa steg att kopiera innehållet. För detta ändamål har det utvecklats diverse mjukvaror och även olika filformat [6, s. 56]. Utan att gå in på de tekniska detaljerna kan nämnas att gemensam nämnare för dessa verktyg och filformat är att de är skapade för att bevara bevismaterialets integritet [15, s. 202]. Ifall valet gjorts att inte kopiera bitströmmen i ett filformat utan rakt till annan lagringsmedia kallas det kloning av data. Proceduren är trots detta den samma, men med det ytterligare kravet att lagringsmedian vart bitströmmen kopieras är ”ren”. En lagringsmedia kan anses ren ifall där inte existerar någon gamla data. I detta fall räcker det inte med att manuellt radera bort alla filer från lagringsmedian, utan det krävs att hela lagringsmedians kapacitet skrivs över med ettor eller nollor [6, s. 56-57][16, s. 5][10, s. 49-50, 137]. Denna procedur säkerställer även att all oallokerad data på lagringsmedian också skrivs över med nya data [16, s. 2].

Oallokerad data innebär data som filsystemet inte mera har i sina register (t.ex. NFST-filsystemets *Master File Table*). Då en fil raderas från filsystemet händer det ingenting med filens data annat än att det inte finns någonting i filsystemet som mera pekar på det. Området filen befinner sig på märks efter detta till ett område vart operativsystemet får skriva in nya data [10, s. 132, 181]. Detta innebär att filens data hålls intakt ända tills nya data skrivs på samma område av hårdskivan. Hårdskivans oallokerade område kan med andra ord innehålla en mängd värdefull information som t.ex. raderade filer vilka kan återskapas i processionsfasen [10, s. 43-44]. Tillgång till oallokerad data är också en av orsakerna till att en bitströmskopia av bevismaterialet är det metodologin förespråkar – då precis all data kopieras får den tekniske undersökaren tillgång till, förutom oallokerade data, även operativsystemsdata.

En bitströmskopia kallas i vissa sammanhang även till en fysisk kopia. Ifall det inte är möjligt att få en fysisk kopia av data är följande alternativ en s.k. logisk kopia. Logisk kopia kan innebära olika saker i olika sammanhang. Ifall filer kopieras rakt ur ett operativsystem som är igång fås en logisk kopia av innehållet. Det innebär att kopian

innehåller endast sådana data som operativsystemet ger användaren tillgång till vilket utesluter bl.a. oallokerade data. Även en enskild kopia av en fil betraktas som en logisk kopia [16, s. 3]. För att få en bekräftelse om att data kopierats på ett tillförlitligt sätt används s.k. kontrollsummor. I följande underrubrik redogör avhandlingen för vad en kontrollsumma innebär.

3.4.1 Kontrollsummor

Eftersom det är viktigt att kunna få en bekräftelse om att kopieringen av data lyckats och att den skett på ett kriminaltekniskt sunt vis har det utvecklats matematiska algoritmer som kallas ’*hashingfunktioner*’. En *hash* kallas i vissa fall även på engelska ’*checksum*’, i denna avhandling använder vi ordet *kontrollsumma* och verbet *hashing* för uträkning av kontrollsumman. Kontrollsumman räknas ut genom att ta i beaktande filens alla bitar och på basis av dem produceras en textsträng som fungerar som en unik id för filen [17, s. 182]. Kontrollsumman är till sin natur deterministisk och unik, vilket innebär att samma fil alltid producerar samma kontrollsumma och två olika filer kan inte producera samma kontrollsumma. Ytterligare måste kontrollsumman produceras så att det inte ska gå att gissa sig fram till den. Detta innebär att ifall en bit ändras i filen ska den nya kontrollsumman fullständigt avvika från den tidigare.

Med hjälp av användningen av kontrollsummor går det att försäkra sig om en lyckad kopiering av en fil. Detta görs genom att granska kontrollsumman av ursprungsfilen mot den kopierade filen, ifall den är den samma innebär det att de två filerna är identiska [17, s. 153, 182-183][10, s. 51]. Dessutom kommer användningen av kontrollsummor ofta till nytta ifall en kriminalteknisk kopia måste undersökas av någon annan teknisk utredare. Då används kontrollsumman för att försäkra sig om att utredaren utgår från samma ursprungsmaterial [6, s. 62].

I dagens läge finns det en mängd olika standardiserade algoritmer för uträkning av kontrollsummor. Av dessa kan nämnas bl.a. MD5 (Message Digest 5), SHA-1 (Secure Hashing Algoritm) och SHA-256. Trots att algoritmerna är väldigt robusta, har olika laboratorium lyckats skapa kollisioner mellan två innehållsmässigt avvikande filer och fått dem att producera samma kontrollsumma. Detta experiment har lyckats med bl.a.

hash-funktionerna MD5 och SHA-1. Som följd av detta har det skapats nya algoritmer för uträkning av kontrollsummor där risken för kollisioner är minimerade, till dessa hör bl.a. den tidigare nämnda kontrollsumman SHA-256 [18, s. 2-3].

Kopiering av digitala bevismaterial lägger grunden för allt vidare arbete i utredningen. Då beviset är på ett korrekt vis kopierat går det alltid att gå tillbaka till startrutan och börja om ifall någonting under processions- eller analysfasen råkar gå fel [6, s. 56].

3.5 Processering digitala bevismaterial

Dagens digitala apparater har en förmåga att lagra stora mängder data och för varje år som går ökar dessa apparaters lagringskapacitet [19]. Detta innebär att redan en minnessticka kan innehålla så mycket material att det vore omöjligt för en kriminalteknisk undersökare att manuellt gå igenom varje fil i den. Till detta ändamål har det utvecklats en mängd olika verktyg för att automatisera processen. Processeringen utgår från data som det gjorts en kriminalteknisk kopia på.

Orsaken till att det digitala bevismaterialet processeras är för att underlätta analysdelen genom att data omformas till en mer lätthanterlig form [20, s. 126-127]. Processeringen av data kan ske helt manuellt men i regel används dedikerad mjukvara för detta ändamål. Orsaken till användningen av mjukvara i processeringsskedet är enkel, en hårdskiva kan innehålla så mycket data att tiden för utredningen skulle bli alltför lång. Manuell procession skulle även kräva en detaljerad kunskap i hur olika filsystem är uppbyggda samt hur olika filformat är definierade [10, s. 49-50]. Dagens mjukvarulösningar söker även automatiskt upp relevanta data som sedan kan analyseras noggrannare [15, s. 307-308]. Trots att automation är nödvändigt i processeringsfasen, ökar också risken för försummande av relevant bevismaterial som mjukvaran inte förstår sig på. [21, s. 5]. Att mjukvaran inte processerar allting är mera regel än undantag. Eftersom det finns ett konstant flöde av nya applikationer på marknaden blir det svårt för mjukvaruutvecklarna att hinna utveckla stöd för varenda applikation. Situationen underlättas inte heller av att det kan ske ändringar i applikationerna i samband med att det lanseras nyare versioner av dem. Processeringen är till för att underlätta och försnabba analysen av materialet och är till

sin natur inte vattentät, metodologin uppmanar därför att alltid själv validera resultaten för sådant som kan senare användas som bevis samt upprätthålla en noggrann dokumentering [21, s. 5, 9].

3.6 Analys av digitala bevismaterial

Analysen av digitala bevismaterial bör fokuseras på att systematiskt gå igenom relevanta data som kan tänkas ha koppling till ärendet som utreds [7, s. 2]15, s. 302]. Detta innebär att undersökningen måste hållas ändamålsenlig och fokuserad eftersom det sällan finns tillräckliga resurser för att kamma igenom all data.

I vanliga fall är målet med analysen följande:

- Utredning av hur data som undersöks har uppkommit, när och av vem/vad.
- Upptäckande av gömda eller krypterade data.
- Att få en uppfattning om användarens tekniska kunskaper.
- Identifiering av aktiviteter på systemet och ifall användaren går att binda till dessa.
- Identifiering av potentiella bevis och dess signifikansnivå på saken som utreds.
- Identifiering av behov av ytterligare bevismaterial eller annan hårdvara som bör undersökas.
- Prövning av olika teorier på bevismaterialet.
- Konstruktion av en tidslinje för relevanta händelser.

Genom att försöka besvara dessa frågor utformar sedan den tekniska undersökaren en hypotes om händelseförloppet som antingen går att bevisa eller i andra fall förkastas med det material som finns till hands [8, s. 5].

En effektiv och korrekt analys kräver alltså mycket av en teknisk utredare. Det krävs kunskap om en mängd olika fil- och operativsystem, filformat och hårdvara. Det i sin tur innebär att en teknisk utredare tvingas hålla sig konstant uppdaterad om det senaste inom branschen [20, s. 122-123]. Utöver detta krävs en förmåga att se på bevismaterialet i sin helhet eftersom digitala bevis är lätta att förfalska. Grovt går det att dela upp data i ett operativsystem i nödvändiga och icke-nödvändiga data.

Nödvändiga systemdata är sådan som krävs för att operativsystemet ska kunna utföra kritiska operationer som t.ex. att öppna och spara filer. Exempel på nödvändiga data är filnamn och pekare på var filen befinner sig i systemet. Icke-nödvändiga data finns till för bekvämlighetens skull men krävs inte för att basoperationerna i operativsystemet ska fungera. Exempel på icke-nödvändiga data är filers tidsstämplar och tillståndsdata. Det är viktigt att kunna skilja åt på nödvändiga och icke-nödvändiga data eftersom nödvändiga data går att lita på, medan icke-nödvändiga data lätt går att förfalskas [10, s. 131].

Ytterligare kräver det att materialet genomgås manuellt för att söka efter potentiell information verktygen missat. Det kan vara fråga om extrahering av filer från hårdskivans oallokerade områden eller identifiering av mera ovanliga filformat på basis av filers filrubriker i hexadecimal-format [10, s. 135-136]. Detta kräver en förståelse över de data som hanteras samt det egna kriminaltekniska laboratoriets kapaciteter. En effektiv analys och tillgång till viss typ av data kan kräva användning av utomstående experter eller specialverktyg [15, s. 311-312].

Liksom i tidigare delar av metodologin är även här dokumentering viktigt. I dokumentering bör framgå exakta versioner på operativsystem och applikationer samt vilka metoder och tekniker den tekniska undersökaren använt sig av för tolkningen av data. Dokumenteringen tjänar även här syftet att möjliggöra återskapande av resultat undersökaren kommit fram till [22, s. 10].

3.7 Valideringsprocessen

Trots att en stor del av relevanta data upphittas med hjälp av verktyg som automatiserar processen, kräver analysdelen ofta att den tekniska undersökaren för hand går igenom materialet för att validera fynden samt hitta sådant verktygen kan ha missat. Inga verktyg kan skapas felfria. Fel i en vetenskaplig kontext innebär inte något som kan undvikas med extra noggrannhet eller försiktighet. Felen kan även delas in i slumpmässiga och systematiska fel. Storleken på slumpmässiga fel kan räknas ut genom statistiken medan systematiska fel härleds från felaktig

implementation av verktyg eller tekniker. Metodologins syfte är minimera risken för systematiska fel samt på ett pålitligt sätt att mäta storleken på de slumpmässiga felen. Vidare kan nämnas att mätningen av de slumpmässiga felen kan vara utmanande då populationen som mäts konstant ändras. Med populationen syftar avhandlingen på diverse mjuk- och hårdvara som i och med teknologins framsteg konstant förnyas [23, s. 7, 10].

Det finns tre primära källor av fel som ofta uppstår vid en undersökning där automatisering används. Den första är ofullständighet, vilket innebär att verktygen inte hittat all relevant information. Den andra är oriktighet, vilket innebär att verktygen representerar data inkorrekt. Tredje felet är feltolkning av data, det innebär att utredaren eller verktyget dragit fel slutsatser på grund av saknande kunskaper eller information [23, s. 3].

För att försöka eliminera dessa fel krävs en valideringsprocess. Under valideringsprocessen bör följande frågor beaktas [23, s. 3-4]:

- Har alla upphittade digitala artefakter de facto sitt ursprung från det analyserade materialet eller har ett defekt verktyg producera nya data?
- Har någon process alternerat data eller gjorts så att informationen representeras felaktigt?
- Är informationen associerad på ett korrekt sätt (e.g. är webhistoriken associerad till rätt webbläsare)?
- Har verktyget tagit i beaktande korrupt data?

För att kunna stå på en stadig grund, måste verktygen som används konstateras vara tillförlitliga. Detta gäller både hårdvara och mjukvara [6, s. 35][24, s. 4]. Valideringen sker ofta i samband med införskaffning av ny hårdvara eller mjukvara eller då befintlig mjukvara uppdateras. I USA har institutionen Scientific Working Group on Digital Evidence (SWGDE) lagt upp följande process för validering version [24, s. 4]:

1. Uppläggning av en testplan som innehåller följande: Avgränsning, vad som ska testas, testningsmetodologin, olika testscenarion och vad som kan tolkas som ett godkänt kontra icke-godkänt test, vad för testdata som och vilka verktyg som används.

2. Testandet utgående ifrån upplagda testscenarion där följande kriterier bör uppfyllas: datasamplet/hårdvaran som testas bör vara i ett känt tillstånd, alla testresultat dokumenteras där det framkommer om resultatet var godkänt eller inte.

Det finns även andra institutioner som regelbundet gör valideringstester på hård- och mjukvara som används inom den digitala kriminaltekniska industrin. Till dessa institut hör bl.a. National Institute of Standards and Technology (NIST) som är baserat i USA. Från NIST:s hemsidor finns tillgång till deras rapporter över testresultat och även datasampel som hjälper en att göra egna valideringstester [25]. Ett typiskt NIST-valideringstest innehåller följande element: beskrivning av det som är föremål för testet samt version/modellnummer, summering av testet, testmiljön, testresultat och testets setup samt verktygens versioner [26]. Av testupplägget går att bekräfta att metodologin är den samma som är upplistad av SWGDE. En väldokumenterad valideringsprocess gör det lätt för andra att försöka reproducera resultaten.

Förutom validering av hård- och mjukvara behöver själva processen samt utförarens kunskaper och slutsatser valideras. Noggrann dokumentering är en förutsättning för att processen ska kunna valideras. Då processen är väldokumenterad kan slutsatserna lättare valideras t.ex. genom en peer review. Detta innebär att en annan utredare försöker reproducera resultaten genom att utföra de åtgärder som är dokumenterade. Samtidigt synas också valda tekniker och verktyg. För att kunna validera andras och egna resultat krävs skolning i både teorin bakom metodologin och användningen av verktygen [6, s. 35][24, s. 5,14].

3.7.1 Bias

Då en annan utredare validerar resultaten minskar risken för att förutfattade meningar (bias) påverkar utredningen i någon riktning. Det har på senaste tiden lagts mer fokus på hur dessa tankefel, även kallade kognitiva bias, kan påverka utredningens gång. Kognitiva bias kan kort förklaras som tankegenvägar vilka sker omedvetet och bör inte förväxlas med tankefel resulterade av medvetna fördomar [27]. Sunde och Dror nämner tre kognitiva bias som speciellt ofta förekommer inom kriminaltekniken:

1. *Ankarbias*: leder till att för mycket tyngd läggs på den första informationen som påträffas och dess betydelsefullhet missuppskattas.
2. *Tillgänglighetsbias*: leder till överskattning av vilka utfall som förväntas baserat på liknande erfarenheter som skett nyligen.
3. *Konformationsbias*: leder till att den tekniska utredaren lägger större tyngd på sådana bevis som understöder utredarens hypotes och lättare förkastar material som motbevisar hypotesen.

Ifall den tekniska utredaren har som uppgift att undersöka digitala bevismaterial för utredningen av ett brott, är det lätt hänt att utredningens fokus blir på att hitta just sådana bevis som förstärker hypotesen om att brottet begåtts medan sådana bevis som talar för det motsatta förbises [27]. Ju mer irrelevant information en teknisk utredare har om fallet, desto lättare händer det att utredarens kognitiva bias börjar spela en roll i undersökningen.

Att blinda den tekniske utredaren för all bakgrundsinformation relaterat till materialet som är föremål för undersökning är ett sätt att förmildra effekterna av kognitiva bias. Detta är dock inte alltid möjligt eller praktiskt. Eftersom en teknisk apparat nuförtiden kan innehålla en mängd data, är utredaren i behov av någon slags kontext för att kunna avgränsa utredningen till relevanta data. Ofta samarbetar de tekniska och taktiska utredarna, vilket lätt leder till att den tekniska utredaren blir exponerad till sådan information som kan ge upphov till förutfattade meningar - både på gott och ont. [27]. För att motarbeta kognitiva bias som uppstår på det här viset, föreslår Dror en metod där det noggrant regleras när, hur och hur mycket information den tekniske utredaren delges. Andra metoder som kan förmildra effekten av kognitiva bias är att den tekniske utredaren tvingas testa många olika hypoteser samt att inte samma person både beslagtar och analyserar de digitala bevismaterialen. Slutligen gäller även här att ha en öppen dokumentering där det även framgår vilka utgångsfakta den digitala utredaren hade under utredningens gång [27].

3.8 Rapportering av fynd

Slutresultatet av en digital kriminalteknisk undersökning brukar oftast presenteras i form av en rapport. Formatet på rapporten varierar beroende på målgruppen och syftet med rapporten, men i regel bör fynden presenteras på ett sådant vis att även en lekman förstår sig på dem [6, s. 9]. Utifrån rapporten ska det också gå att få en helhetsbild över vilka metoder, verktyg och tekniker som använts samt vilka objektiva slutsatser som kan dras på basis av utredningen [20, s. 127]. Det måste även framkomma relevant information om bevismaterialet, som t.ex. hårdvarans modell eller vilken version av applikationen som undersökts. Resultaten ska även presenteras på ett sådan vis att de kan återskapas. Till rapporten kan även bifogas data som används i bevisningssyfte, men i de flesta fall räcker det med en beskrivning om var och hur data som används som bevis kan hittas [28, s. 216].

Ytterligare bör läggas fokus på rapportens uppbyggnad och hur den är organiserad. Stilmässigt bör texten hållas kort och koncist samt hålla fokusen på det som är relevant. För att underlätta läsningen hjälper det att inleda med en summering av fynden och utredningens slutsatser [28, s. 62-63][15, s. 581]. Användning av ordlistor för att förklara obekant terminologi kan också vara till stor nytta för läsaren av rapporten [29, s. 11].

Rapporten är alltså ett dokument vart information som tagits upp i alla metodologins olika faser destilleras till en helhet. Ifall de olika skedena i metodologin lämnats odokumenterade eller dokumenteringen är bristfällig kommer detta högst sannolikt att reflektera över den slutgiltiga rapporten. Detta i sin tur kan i värsta fall innebära att en stor del av arbetet går till spillo ifall personerna som läser rapporten inte lyckas ta till sig texten [28, s. 217].

4. Diskussion och sammanfattning

Bevis och tillvaratagande

Ur litteraturen kan konstateras att digital kriminalteknisk undersökning innefattar en mängd olika steg ämnade för att bevara integriteten på bevisen, men frågan återstår ifall dessa är tillräckliga för att bevara digitala bevisens integritet.

Till skillnad från den traditionella kriminaltekniken kan konstateras att den digitala kriminaltekniken inte ännu är lika robust och håller ännu på att ta sin form. Eftersom lagstiftaren bestämmer under vilka premisser en digital kriminalteknisk undersökning får utföras, är det naturligt att vissa delar i metodiken skiljer sig mellan olika länder. Största skillnaderna hittas i kraven på bevisföringen och tillvaratagandet av bevis.

Jämförs länder som Finland och USA framkommer det tydligt hur mycket tyngd lagstiftaren i USA lägger på bevismaterialets spårbarhet (eng. *chain-of-custody*). Detta framkommer även i litteraturen, där metodologin ur USA:s synpunkt ofta betonar hur ett bevis kan förkastas ifall det finns luckor i spårbarheten. I Finland, var domstolen har fri bevisprövning, betonas det mer hur bevismaterialet i sin helhet ska kunna anses tillförlitligt och detta avgörs av domstolen. Trots det poängterar finska lagstiftningen i en mindre specifik form, att de åtgärder som utförs under utredningen inte får påverka bevismaterialets integritet.

Lagstiftaren har heller inte tagit större ställning vad kraven på hur ett korrekt tillvaratagande av fysiska bevismaterial ska se ut. I tvångsmedelslagen kap 8 §22 står det kort att en polisman har rätt att omhänderta en teknisk anordning för genomsökning, men här saknas vidare utveckling om hur detta måste ske för att säkra ägarens rättsskydd. Detta leder lätt till en stor variation mellan hur olika bevismaterial beslagtas, vilket i sin tur kan påverka bevisets integritet.

Identifiering av bevis

I delen om identifiering av digitala bevismaterial försöker metodiken på ett mera allmänt plan väcka tankar om vad som i dagens värld potentiellt kan innehålla viktiga data. Eftersom det hela tiden utvecklas nya teknologiska apparater är det onödigt att

försöka göra en uttömmande lista på dem, utan istället försöka uppmuntra utövare av digital kriminalteknik att hålla sig uppdaterade inom området. Vad metodiken kunde poängtera mer, är hur kognitiva bias kan påverka vilka typer av digitala bevis som slutligen konfiskeras. Nina Sunde belyser problemet i sin vetenskapliga artikel, där det framkommer i studier att utredningens natur kan orsaka förutfattade meningar hos den tekniska utredaren, vilket i sin tur har en inverkan på bevisets integritet.

Kopiering

En kriminalteknisk kopia är det närmaste den digitala kriminaltekniken kommer den traditionella kriminalteknikens DNA prov i fråga om vetenskapligt beprövade och robusta metoder. I och med att kopians integritet kan bekräftas med matematiska algoritmer för uträkning av kontrollsummor, kan det läggas stor tillit till metoden. Trots att själva kriminaltekniska kopians integritet är lätt att bekräfta, kräver det att de steg i metodologin som kommer före kopieringen har följts. Kontrollsumman berättar ingenting om data som alternerats, medvetet eller omedvetet, innan kopian togs. Här finns alltså utrymme för fusk och misstag vilket betonar vikten på utförlig dokumentation genom hela processen. En välgjord dokumentering medför en öppenhet och genomskinlighet, vilket underlättar bedömningen av bevisets integritet. En kriminalteknisk kopia är även förutsättningen för att hela analysen och processeringen av materialet ska kunna återskapas.

Processering, analys och validering

På grund av att mängderna data i diverse digitala utrustningar ökar för varje år har ett behov av automatisering uppstått. Detta i sin tur har öppnat en marknad för olika företag att lansera produkter ämnade för processering av digitala bevis. Det är dock omöjligt att utveckla en sådan produkt som förstår sig på all form av data eller en produkt som inte innehåller några fel. En kriminalteknisk utredning kan innehålla material från flera olika apparater och tidskraven på utredningen kan även vara stränga. Denna kombination medför en risk där det läggs en alltför stor tillit på de automatiserade resultaten verktyget framställt. Därför poängteras det i metodiken att de resultat som presenteras även ska valideras manuellt av kriminalteknikern. Här

framhäver Carrier skillnaden mellan data som är nödvändiga och icke-nödvändiga för ett fungerande filsystem, där det sistnämnda är sådan data det inte går att lite på blint. Här finns alltså många fallgropar en kriminaltekniker kan gå på. Det är inte ovanligt att det i samband med ett digitalt bevismaterial presenteras tidstämplar som berör bevismaterialet. En tidsstämpel i sig räcker inte enligt Carrier ensamt som bevis, utan det krävs att tidsstämpeln bekräftas med övriga data. En förståelse över de automatiska verktygens styrkor och svagheter är alltså en nödvändighet för att bevisens integritet ska bevaras.

Metodologin föreslår att analysen planläggs där det framkommer vad som skall utredas, hur det skall utredas och med vilka verktyg. Efter planeringen prövas olika hypoteser på bevismaterialet – hypoteserna kan sedan bekräftas, förkastas eller förbli obesvarade. Under analysen kan det också framkomma brister i det material som samlats in vilket kan ge upphov till ett behov av ytterligare bevisinsamling. En välgjord analys kräver ofta mycket manuellt arbete med data samt att en mångfald av hypoteser prövas. Analysen bör dokumenteras på ett sådant vis att en utomstående kan få en förståelse över vad och varför någonting analyserats samt vilka hypoteser som prövats. Endast då går det att upptäcka potentiella brister i analysen eller kriminalteknikers kunskaper samt att få förståelse över materialet som analyserats.

Varje resultat i analysen måste även kunna bekräftas och valideras. Själva valideringsprocessen börjar i själva verket innan analysen, då de verktyg som används för hanteringen av bevisen valideras för att kontrollera att de faktiskt fungerar och producerar tillförlitliga resultat. Hur valideringsprocessen är uppbyggd varierar beroende på vad som skall valideras, men som SWDGE nämner i deras akademiska papper angående validering är det väsentligt att innan själva valideringsprocessen specificera vad som skall testas, hur det skall testas, med vilka testdata och med vilka verktyg. Hela processen bör sedan noggrant dokumenteras och resultaten antecknas.

Rapportering

Hela den digitala kriminaltekniska utredningen presenteras allt som ofta i form av en rapport. Då rapporten skrivs måste skribenten vara medveten om vem eller vilka som kommer att läsa den. Eftersom en teknisk utredning underförstått innehåller en mängd tekniska termer, måste dessa förklaras på ett sådant vis att även en lekman förstår.

Trots detta krav bör rapporten vara tillräckligt detaljerad, så att en utomstående tekniker i behov kan återskapa resultaten.

Ifall det inte läggs tillräckligt tanke och omsorg till rapporteringen av fynden, kan det leda till missförstånd i sakens vidarebehandling. Detta i sin tur kan i värsta fall ha en inverkan på bevisens integritet.

Sammanfattning

Sammanfattningsvis kan konstateras att metodologin i sin helhet ger en stabil grund för utförande av digital kriminalteknik. I varje steg tar metodologin ställning till hur processen reflekteras på bevisens integritet och hur undersökningen hålls öppen för utomstående ögon. Trots att metodologin kan anses vara robust, finns de naturligtvis rum för förbättring. Att standardisera sättet de olika skeden dokumenteras kunde göra undersökningarna mer enhetliga och även förminska risken för en kriminaltekniker att missa något viktigt steg i processen.

4.1 Förslag till fortsatt forskning

Denna avhandling undersökte hur metodologin inom digitalkriminalteknik inverkar på bevismaterialens integritet. Metodologin har en teknisk inriktning där olika fallgropar och problem försöker lappas med tekniska lösningar. Utöver det tekniska lösningarna skulle en mer medveten satsning på den psykologiska delen vara aktuell. Eftersom digital kriminalteknik sist och slutligen utförs av människor, går det inte att förbise att psykologiska faktorer omedvetet kommer att inverka på hur arbetet utförs. Kognitiva bias kan bevisligen få en utredare att producera falska resultat.

REFERENSER

Konferenser:

[1] Digital Forensic Reasearch Conference, "A Road Map for Digital Forensic Reasearch", The Digital Forensic Reasearch Conference, 2001.

Myndighetspapper:

[2] Europeiska kommissionen, Neuvoston päätös: "luvan antamisesta aloittaa neuvottelut sopimuksen tekemiseksi Euroopan unionin ja Amerikan yhdysvaltojen välillä oikeudelliseen yhteistyöhön rikosasioissa liittyvästä rajat ylittävästä pääsystä sähköiseen todistusaineistoon", 2019. [Online]. Tillänglig på: https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:52019PC0070&from=EN. [Besökt 2.3.2021].

[29] Association of Chief Police Officers, Good Practice Guide for Digital Evidence, 2012.

Böcker:

[3] H.T Klami, Todistusratkaisu, Helsinki: Lakimiesliiton kustannus, 2000.

[5] J. Jonkka, Todistusharkinnasta, Helsinki: Lakimiesliiton kustannus, 1993.

[6] J. Sammons, The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics¸ 2nd ed., Syngress publications, 2015.

[10] B. Carrier, Filesystem Forensic Analysis, Addison Wesley Professional, 2005.

[15] J.T. Luttgens, M. Pepe, Incident Response & Computer Forensics, 3rd ed., McGraw-Hill Education, 2014.

[17] Y. Lindell, J. Katz, Introduction To Modern Cryptography, 2nd ed., Crc Press, 2018.

[28] M.G. Solomon, K. Rudolph, E. Tittel, N. Broom, D. Barret, Computer Forensics Jumpstart, 2nd ed., Wiley Publishing Inc., 2011.

Journaler:

[4] D. Frände, ”Tuomitsemiskynnyksestä suomalaisessa rikosprosessioikeudessa”, Lakimies, s. 1247-1254, nr. 8, 1998.

[7] M. Reith, C. Carr, G. Gunsch, ”An Examination of Digital Forensic Models”, International Journal of Digital Evidence, vol. 1, nr. 3, 2002.

[8] S.R. Selamat, R. Yusof, S. Sahib, ”Mapping process of Digital Forensic Investigation Framework”, IJCSNS International Journal of Computer Science and Network Security, vol. 8, nr. 10, s. 163-169, 2008.

[20] A. Agarwal, M. Gupta, S. Gupta, S.C. Gupta, ”Systematic Forensic Investigation Model”, International Journal of Computer Science and Security, vol. 5, nr. 1, s. 118-136, 2011.

[27] N. Sunde, I.E. Dror, Cognitive and human factors in digital forensics: Problems, challenges, and the way forward, Elsevier, 2019.

Instituts och organisationers webbplatser:

[9] National Institute of Standards and Technology, ”Digital Evidence”. [Online]. Tillgänglig på: https://www.nist.gov/digital-evidence. [Besökt: 5.2.2021].

[12] International Organization for Standardization, ”ISO/IEC 27037:2012”. [Online]. Tillgänglig på: https://www.iso.org/standard/44381.html. [Bestökt 27.3.2021].

[13] P. Henry, ”Best Practices In Digital Evidence Collection”, SANS, 2009. [Online]. Tillgänglig på: http://www.sans.org/blog/best-practices-in-digital-evidence-collection. [Besökt: 27.3.2021].

[25] Homeland Security. [Online]. http://www.dhs.gov/science-and-technology/nist-cftt-reports. [Besökt: 27.3.2021].

Artiklar på webben:

[19] Frontierinternet.com, ”Data Storage Devices”. [Online]. Tillgänglig på: https://www.frontierinternet.com/gateway/data-storage-timeline. [Besökt: 27.3.2021].

Akademiska papper:

[11] Scientific Working Group on Digital Evidence, Best Practices for Digital Evidence Collection, 2018.

[14] Scientific Working Group on Digital Evidence, Capture of Live Systems, 2014.

[16] S. Vandeven, Forensic Images: For Your Viewing Pleasure, SANS, 2014.

[18] S. Halevi, H. Krawczyk, Randomized Hashing and Digital Signatures, IBM T.J Watson Research Center, 2007.

[21] Scientific Working Group on Digital Evidence, Best Practices for Computer Forensic Aquisitions, 2018.

[22] Scientific Working Group on Digital Evidence, Best Practices for Mobile Device Forensic Analysis, 2020.

[23] Scientific Working Group on Digital Evidence, Establishing Confidence in Digital and Multimedia Evidence Forensic Results by Error Mitigation Analysis, 2018.

[24] Scientific Working Group on Digital Evidence, Recommended Guidelines for Validation Testing, 2014.

Tekniska rapporter:

[26] Department of Homeland Security and Technology Directorate Cyber Security Division by the Office of Law Enforcement Standards of the National Institute of Standards and Technology, ” Tableau eSATA Forensic Bridge T35es-R2”, USA, 2013.