HÖGSKOLAN I HALMSTAD

IT-forensik och informationssäkerhet 180 hp

KANDIDATUPPSATS

Anti-forensik

Anti-forensiska metoder på mobila enheter

Hans Bade och Oscar Hedlund

Digital forensik 15 hp

Halmstad 2018-05-31

Anti-forensik

Anti-forensiska metoder på mobila enheter

Hans Bade, Oscar Hedlund

Kandidatuppsats

May 31, 2018

© Hans Bade, Oscar Hedlund 2018
Akademin för informationsteknologi
Högskolan i Halmstad

Abstrakt

Mobiltelefoner har blivit grundläggande för extrahering av digitala artefakter i forensiska utredningar. Androids Linuxbaserade operativsystem medför större möjligheter för anti-forensiska metoder, detta gör att kunskap om anti-forensik är essentiell för dagens IT-forensiska utredare. I denna studie belyses effekten av anti-forensik i Androidbaserade mobila enheter samt så upplyses det om dagens anti-forensiska attack metoder mot forensiska verktyg. Genom experiment så visas det hur man kan förhindra ett forensisk verktyg från att extrahera data med användning av ett simpelt script.

Abstract

Mobile phones have become essential for the extraction of digital artifacts in forensic investigations. Android's Linux-based operating systems bring greater potential for anti-forensic methods, which means that knowledge of anti-forensics is essential to today's IT forensic investigators. In this study, the effect of anti-forensics on Android-based mobile devices is highlighted, as well as revealing today's anti-forensic attack methods against forensic tools. By experiment, it is shown how to prevent a forensic tool from extracting data by using a simple script.

Definitioner

Root

Den högsta behörighetsgraden i ett system.

Zero-day exploit

En attack som utnyttjar en, för utvecklaren, tidigare okänd sårbarhet i mjukvara eller hårdvara.

Filsignatur

Data som identifierar en fils filformat.

SELinux

Akronym för Security-Enhanced Linux, som instruerar säkerhetspolicy i Linux-baserade miljöer.

Script

text som innehåller instruktioner el. kommandon till dataprogram.

Innehåll

Figurer

1 Introduktion

Digital forensik har blivit av stor vikt på senaste åren då digitalisering av information kraftigt växt, till stor del med hjälp av att mobila enheter används i allt större utsträckning. Enligt GSMA Intelligence, forskningsavdelningen av mobiloperatörernas organisation GSMA, finns det över fem miljarder unika mobila enheter i världen [1].

Det har skapat en stor marknad för digitala forensiska verktyg som underlättar det forensiska arbetet och beroendet på dem har ökat med tiden. Naturligtvis finns det även de som vill försvåra det forensiska arbetet, därför har en mängd anti-forensiska metoder uppstått, ofta med huvudmålet att hindra inhämtning av bevismaterial i forensiska undersökningar [2]. Många av dessa metoder är tillgängliga för allmänheten och kräver endast minimal teknisk kompetens för att användas. Sporea et al. beskriver i sitt arbete [3] ett flertal applikationer som finns tillgängliga för allmänheten på Androids ”Play Store” respektive Apples ”App Store” som enkelt kan utföra olika anti-forensiska tekniker.

Eftersom anti-forensik är ett så pass nytt område finns det ingen globalt accepterad definition [2][4], det finns istället en mängd olika definitioner som ofta är specifika för de områden som undersöks.

Exempel på definitioner som finns är följande:

> ”*Attempts to negatively affect the existence, amount and/or quality of evidence from a crime scene, or make the analysis and examination of evidence difficult or impossible to conduct.*”

Marc Rogers definition [5] är utformad på en mer traditionell tillvägagångssätt då den hänvisar anti-forensik som en brottsplats och inte tar med bevaring av personlig integritet.

På samma sätt sammanfattar Scott Berinato [6] definitionen av anti-forensik på följande vis:

> ”*Make it hard for them to find you and impossible for them to prove they found you.*”

I Ryan Harris arbete ”Arriving at an anti-forensics consensus” [4] definieras dock anti-forensik som:

> ”*any attempts to compromise the availability or usefulness of evidence to the forensics process*”

Det är den definition detta arbete arbetar utifrån då den är väl hänvisad inom anti-forensiska forskningsområdet då författaren har kombinerat tidigare definitioner för att kunna ha med alla aspekter inom anti-forensik i tanke och även håller definitionen kort så den kan standardiseras.

I samband med att allas digitala säkerhet och integritet har fått mer och mer uppmärksamhet har även dessa anti-forensiska metoder börjat användas allt flitigare. Exempelvis kan kryptering av datan på datorer och mobiltelefoner möjliggöras med hjälp av funktioner som finns förinstallerade med de flesta operativsystem. Dessa nya tekniker har gjort att forensiska processen och synen på tillvägagångssättet förändrats, till exempel innebar den ökade användningen av krypterade system att man slutade använda ”pull the plug” metoden [7].

Ett väldigt uppmärksammat fall på senare tid där förinstallerade anti-forensiska tekniker försvårade utredningen är efter skjutningen i San Bernardino, där Syed Rizwan Farook och hans hustru dödade 14 personer och skadade 22. Polisen hittade i efterhand Syeds iPhone 5C men kunde inte använda den i utredningen på grund av anti-forensiska metoder som fanns förinstallerade. Telefonen i fråga var låst med en fyra-siffrig kod och på grund av kryptering samt hårddiskrensning vid flertalet misslyckade inloggningsförsök kunde FBI inte komma åt informationen. Detta ledde till att FBI tog Apple inför rätta och försökte tvinga dem att skapa bakdörrar till telefonen som FBI kunde använda sig av. Som tur var hittade FBI ett annat sätt att komma över informationen innan dagen för rättegången ägde rum, genom att använda en så kallad zero-day exploit [2].

FBI är långt från ensamma i världen att råka ut för dessa problem, bland annat har det ökade användandet av kryptering inneburit stora problem för olika auktoritära nationer när de försöker kontrollera vad som skickas via internet. Även andra delar av världen går en svår balansgång mellan den personliga integriteten online som kryptering möjliggör och problemen den kan skapa när säkerhetsmydigheter försöker hålla koll på kriminella nätverk och potentiell terrorism. Frågan om privat-

personer ska få använda kryptering av militärkvalitet väcks med jämna mellanrum efter terrorattacker och andra fruktansvärda brott som diverse intresseorganisationer och politiska partier tycker sig kunna förebygga genom mer övervakning av befolkningen. Stark kryptering har inte förbjudits i största delen av världen så det är, och kommer i framtiden förmodligen fortfarande vara ett stort problem för forensiska analyser.

Forensiska arbeten på mobila enheter är i grunden mer komplicerade än de gjorda på till exempel PCs, detta för att de ofta är byggda på komponenter som inte följer någon standard och använder sig av mjukvara som är proprietär, odokumenterad och som kan ändras ofta [8]. På grund av problematiken det medför har både polismyndigheter och andra organisationer, av tid- och kostnadsskäl, valt att presentera riktlinjer där det rekommenderas att personen som utför den forensiska analysen manuellt ska navigera genom mobiltelefonen[9, 10]. Ett sådant beteende kan skada integriteten på bevismaterialet om inte forensikern har full kännedom om konsekvenserna av dess handlingar. Detta medför att forensikern förlitar sig väldigt mycket på att mobiltelefonens mjukvara fungerar som förväntat vilket kan utnyttjas av personer med anti-forensiska mål. Vidare kan anti-forensiska tekniker problematisera automatiserade forensiska processer [11].

1.1 Bakgrund

Anti-forensik inom IT som forskningsområde är ett relativt nytt ämne, men det betyder inte att anti-forensik inte har förekommit innan. På samma sätt som kriminella gör sitt bästa för att städa igen sina spår när det begås inbrott, våldsbrott och liknande har även IT-brottslingar försökt städa igen sina spår. Det finns en mängd olika, mer eller mindre komplicerade, metoder för att hindra andra från att upptäcka eller kunna bevisa att de begått brottet. Något så trivialt som att använda handskar när ett brott begås kan jämföras med att använda ett Virtuellt Privat Nätverk (VPN) för att det ska bli svårare för utredarna att upptäcka vem som begått brottet. Att förstöra bevismaterial som används kan jämföras med att skriva över informationen på en enhet för att det ska bli svårare att bevisa vilken person som begått brottet.

1.1.1 Definition

Definitionen av anti-forensik är som tidigare nämnt väldigt skild mellan olika författare inom området, på liknande sätt är definitionen om vad som landar inom anti-forensikens ramar. Ryan Harris [4] delar upp anti-forensik i fyra delar: Förstöra bevis, gömma bevis, eliminera beviskällor samt förfalskning av bevis. Garfinkel [12] lade till anti-forensiska tekniker som exploaterade buggar i forensiska verktyg samt tekniker som upptäckte forensiska verktyg, dessa definitioner i sig är väldigt breda och kan även innefatta tekniker och verktyg som inte där intentionen är att vara anti-forensiska. Exempel på sådana tekniker kan vara sådant som stärker integriteten och konfidentialiteten, som VPN och kryptering [2].

För att göra det enklare för forensiker att identifiera anti-forensiska tekniker som andra råkat ut för tidigare är det viktigt att det finns mer specifika och väl definierade kategorier för att möjliggöra spridning av kunskap och bättre begränsningsstrategier. Därför föreslog Conlan et al. [2] sin förlängda anti-digitalforensiska taxonomi där kategoriseringen ser ut som följande:

- Data Hiding

  Detta innefattar metoder som kan dölja data och försvåra forensiska analyser, exempelvis så är kryptering ett sätt att gömma data men också steganografi som gör det svårt att upptäcka gömd data. Ett annat sätt att gömma data är genom manipulation av systemets filstruktur.

- Artifact wiping

  Detta är användningen av verktyg som har som avsikt att förstöra databevis för att försvåra forensiska analyser.

- Trail obfuscation

  Metoder som har som avsikt att vilseleda forensiska undersökningar. Detta kan göras med hjälp av missinformation genom användning av exempelvis spoofing metoder.

- Attacks against forensic tools and methods

  Dessa metoder har potentialen att vara de mest destruktiva mot forensiska undersökningar eftersom attacken sker direkt mot forensiska verktyg samt riktlinjer.

- Possible indication of anti-digital forensics

  Indikationer på att anti-forensik använts, exempelvis så kan installationsfiler för krypteringsverktyg vara en indikation på att det kan finnas krypterad data i systemet.

Inom dessa kategorier finns även en mängd underkategorier, dessa är inte nämnda här på grund av det stora antalet. Eftersom detta arbete kommer att fokusera på anti-forensiska metoder mot IT-forensiska verktyg så kan det vara relevant att nämna de underkategorier som kommer vara mest centrala i denna rapport. Dessa är kategorierna som fokuserar på attacker mot IT-forensiska verktyg.

- Attacks against forensic tools and methods
  - Alerts to forensic tool usage
  - Anti-reverse engineering
  - Forensic software integrity attacks
  - Hash value integrity attacks
  - Investigator integrity attacks
  - Program packers

1.1.2 Relaterade arbeten

Ett arbete som visar på möjligheterna för anti-forensik mot IT-forensiska verktyg är Karlsson och Glissons arbete om anti-forensik på telefoner med operativsystemet Android [8]. De belyser en del av de problem som kan uppstå när en forensiker undersöker en mobiltelefon där ändringar i operativsystemet gjorts, bland annat påpekar de hur IT-forensiska verktyg förlitar sig på att mobilens mjukvara returnerar korrekt data. Detta utnyttjar de för att presentera falsk information för de IT-forensiska verktygen Cellebrite och XRY. Detta gör de genom att modifiera operativsystemet CyanogenMod.

Xiaosong ZhangYu-an Tan et al. [13] visar att det går att skydda vissa processer från att kunna utvinnas med hjälp av IT-forensiska program, i sitt arbete testar de mot verktyget FROST. De gör detta genom att flytta processerna till ett speciellt minnesområde där kärnan laddas. Deras tester visar även att det inte påverkar processernas vanliga funktionsförmågor, deras metod kan även skydda större mängd data än andra liknande metoder.

Meffert et al. [14] undersöker och belyser problem som kan uppstå när forensiska verktyg inte utsätts för tillräckligt med säkerhetstester av tillverkaren. Detta är ett stort problem då integriteten av bevismaterial och diskavbilder är av mycket stor betydelse för forensiska verktyg. I arbetet testar de TD3, en mobil enhet med pekskärm som bland annat kan avbilda hårddiskar. De designade en attack så att de fick root-tillgång till enheten och kunde då ändra uppdateringar till firmware samt köra script på enheten som skadade desinationshårddiskens integritet.

Även attacker som inte riktar sig specifikt mot IT-forensiska verktyg kan även de skapa stora problem för utredare. I Gül och Kugu's arbete A Survey On Anti-Forensics Techniques [15] presenterar de flera anti-forensiska tekniker, bland annat icke-standard RAID:ade hårddiskar, manipulerande av filsignaturer och hash-kollisioner. De presenterade även förslag för att mitigera dessa tekniker.

I arbetet Anti-Forensic Trace Detection in Digital Forensic Triage Investigations [16] belyser de en signaturbaserad metod för detektering av anti-forensiska spår i misstänkta digitala enheter Detta kan hjälpa utredare ta beslut och förebygga att möjlig anti-forensik skadar utredningen innan de påbörjar den.

I arbetet A Novel Anti-forensics Technique for the Android OS [17] föreslås en ny teknik för att säkert och selektivt ändra eller radera digitala bevis på androidenheter utan användning av kryptografiska metoder eller ändringar till filsystemet. Vanligtvis skapas det stora misstankar vid forensiska analyser om kryptografiska metoder eller ändringar på filsystemet upptäcks. Detta gör de genom att använda sig av två olika partitioner på mobilen, flytta datan fram och tillbaka mellan dessa och sanitera partitionen som datan flyttats från.

Sporea et al.[3] testade olika appar från App- och Play Store som förstörde, gömde eller förfalskade data mot forensiska verktygen Device Seizure och Oxygen Forensic Suite. Bland annat testade de applikationerna StegDroid på Android och Fake Location på iPhone. StegDroid låter en användare att gömma ett textmeddelande i en ljudinspelning och kryptera det så endast en person med nyckeln kan läsa det. Fake Location låter användaren ändra mobilens position för olika appar, så att till exempel inlägg på Facebook visar att de skrivits på andra platser. Både Device Seizure och Oxygen Forensic Suite hade problem med att upptäcka att ett meddelande gömts i ljudfilen eller att mobilens position hade ändrats manuellt.

1.2 Syfte

Syftet med studien är att belysa de problem som kan uppstå vid en forensisk analys av mobila enheter samt hur man kan arbeta för att motverka dessa problem. Därav få bättre förståelse för olika anti-forensiska exempel och mitigeringsstrategier.

2 Problemformulering

Med tanke på de tidigare nämnda problem som kan förekomma under en forensisk analys när anti-forensik används, är problemställningarna till denna studie som följer:

- Kartläggning av anti-forensiska metoder mot IT-forensiska verktyg
- Vilken effekt har dessa på digitala forensiska utredningar när de tillämpas på mobila enheter?
- Hur kan anti-forensik i mobila enheter motverkas?

2.1 Problemdiskussion

Flera tidigare arbeten har visat på problem som anti-forensik kan skapa, väldigt få visar dock på hur en forensiker kan förebygga att utredningar drabbas av anti-forensiska attacker. Gül och Kugu [15] tar upp den problematiken och beskriver kortfattat hur de tekniker de presenterar kan motverkas, även Garfinkel [12] beskriver hur tekniker kan motverkas. Ingen av dessa arbeten fokuserar dock på mobila enheter eller attacker särskilt riktade mot IT-forensiska verktyg. Konsekvenser som kan uppstå när anti-forensik påverkar en forensisk utredning nämns i en mängd tidigare arbeten [18, 19], men i denna studie visas det genom ett experiment hur enkelt det kan utföras.

Kartläggningen av anti-forensiska metoder kan vara ett problem om inte tillräcklig information hittas, då mängden forskning inom ämnet är relativt liten. Därav kan det vara att dessa metoder inte finns skrivna i forskningsarbeten. Då kan hänvisning till exempelvis blogginlägg vara nödvändigt, även om de saknar samma pålitlighet.

Effekten som dessa metoder har på IT-forensiska utredningar kan tolkas på olika sätt, det är därför viktigt att hålla sig till den konkreta effekten relaterad till metoden för att hålla det så relevant som möjligt.

Ett stort problem är kunskapsnivån som kan krävas för att motverka vissa metoder. Det är inte bara ett problem för arbetet men även för utredare. Exempelvis

så anses kryptering som en anti-forensisk metod, och detta kräver höga kunskaper inom matematik för att få en djupare förståelse.

2.2 Etik

Inom forensik bemöts man med etiska dilemman vid varje tillfälle. Eftersom anti-forensik kan användas både för kriminella syften och för konfidentialitetsbevaring, är det svårt att bestämma etiska grunder för anti-forensisk forskning. Exempelvis kan kryptering ses som en typ av anti-forensik då den försvårar framställningen av data. Detta kan användas för brottsliga syften, men också för att bevara konfidentialiteten på känslig data. Forskning inom detta blir känslig då resultat kan användas för oetiska ändamål. Eftersom detta arbete avgränsar sig till attacker mot IT-forensiska verktyg, är syftet att få en bättre förståelse på hur man ska bemöta och förhindra dessa tekniker, då attacker mot dessa verktyg nästan alltid har kriminella syften. Eftersom dessa tekniker kan användas av kriminella för att förhindra forensiska utredningar så är det viktigt att få bättre förståelse på hur dessa metoder fungerar och därav kunna få bättre kunskap om hur dessa kan förhindras.

3 Metod

Denna forskning utförs genom att göra en kartläggning av attacker mot IT-forensiska verktyg från mobila enheter samt en empirisk studie på resultatet av kartläggningen. Därmed en undersökning av tekniker och metoder mot IT-forensiska verktyg, samt hur detta påverkar forensiska analyser av mobilenheter. Det kommer även utföras experiment för att visa på effekten av dessa mot IT-forensiska verktyget XRY.

3.1 Metoddiskussion

Tidigare forskningsarbeten har ofta fokuserat på två skilda aspekter, antingen att översiktligt beskriva olika anti-forensiska metoder [12] [15] eller att utveckla och testa sina egna tekniker [8] [14] [13]. Detta arbete menar att sammanföra dessa två områden och på så sätt få en bättre helhetsbild över ämnet. Eftersom arbetet lägger stor vikt på just anti-forensiska metoder mot IT-forensiska verktyg är målet att göra en övergripande kartläggning om flera av de metoder som kan hittas i diverse forskningsrapporter samt andra källor, samt utveckla och testa en egen anti-forensisk teknik. Med hjälp av en empirisk studie kan denna rapport göra de experiment som anses vara av värde för rapporten och producera egna resultat som kan användas för vidare reflektering.

Problem som kan uppstå är att det finns anti-forensiska tekniker som det inte finns någon uppenbar lösning för, eller lösningar som inte löser problemet på ett effektivt sätt.

Det är även möjligt att det inte finns tillgång till kommersiella forensiska verktyg och därmed inte får en bra helhetsbild när vi utför experimenten. Brist på bra dokumentation av både forensiska och anti-forensiska verktyg och metoder är något som kan bli ett problem för att få en bättre förståelse om hur dessa tekniker fungerar. Ett annat problem som skulle kunna uppstå är ifall anti-forensik inte går att detektera, och därmed blir svår att motverka. Andra problem som kan uppstå är att det kan vara svårt att utföra en del av de anti-forensiska teknikerna då det inte alltid finns klara direktiv i hur de utförs, detta kan skapa resultat i experimenten som inte är korrekta.

3.2 Avgränsningar

Vi valde att avgränsa oss till det Androidbaserade operativsystemet LineageOS då det är väldokumenterat och bygger på Android som är open-source som därmed gör det lättare att arbeta med i jämförelse med mer slutna operativsystem som IOS. Vi valde att använda det IT-forensiska verktyget XRY då det är det kommersiella verktyget som det fanns tillgång till. Det är även ett bra val då XRY är ett av de verktyg som svenska myndigheter använder sig av [20]. Underkategorin attacker mot IT-forensiska verktyg valdes inom anti-forensik då det är ett ämne som vi anser kräver mer uppmärksamhet.

4 Experimentuppställning

Experimentet utförs på en mobiltelefon av modellen OnePlus 2 med operativsystemet LineageOS version 15.1 [21]. Valet av OnePlus 2 som telefon är för att det var den telefon som var i bäst skick av de som fanns tillgängliga att experimentera på. LineageOS valdes då det är ett av de mest använda Androidbaserade operativsystemen som finns tillgängliga. Att operativsystemet som används i experimentet är tillgängligt för alla är väldigt viktigt för att det ska kunna upprepas samt att man inte ska få olika resultat beroende på att man använder sig av ett annat Androidbaserat operativsystem. Version 15.1 menar att det bygger på Androids nyaste version - 8.1, även kallat Android Oreo. Detta innebär också att experimenten kommer ske med den senaste tillgängliga säkerhetsuppdateringen från Android. Mobilen använder sig av återställningsläget TWRP [22] för att få lite extra funktionalitet så som ett grafisk gränssnitt samt ytterligare information. TWRP används också då den har stöd flera modeller av mobil enheter, vilket är viktigt för att kunna reproducera experiment.

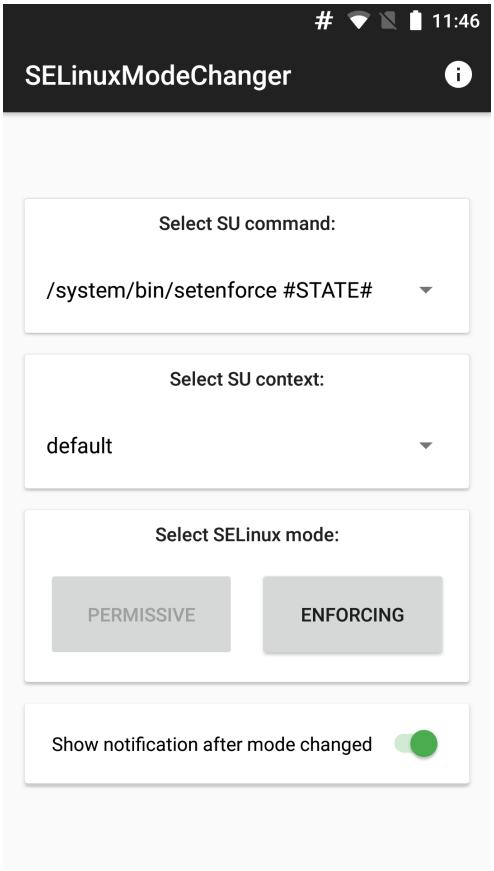
Ett dataset skapas inför experimentet för att kunna kontrollera att det forensiska verktyget fungerar som förväntat. Datasetet består av diverse bilder och andra filer som skapats själva.

Första steget som görs är att installera LineageOS samt överföra datasetet som kommer att finnas på mobilenheten inför experimentet.

Steg två är att skapa en logisk avbild av mobiltelefonen med XRY utan att ha applicerat några anti-forensiska tekniker på den, detta för att se hur mycket och vilken data som kan avbildas under normala omständigheter för att sedan kunna jämföra avbilder med anti-forensiska tekniker på enheten.

Steg tre är att få root-åtkomst på enheten genom att köra programmet SUaddon som finns tillgänglig på LineageOS hemsida. Detta körs i återställningsläge.

Steg fyra är installation av appen SELinux Mode Changer [23] samt applicerande av vårt script i mappen /system/etc/init.d/, scriptet kan ses i Figur 2. Script som är placerade i denna mapp startar vid uppstarten av enhetens operativsystem. Inställningarna i SELinux för enheten som används kan ses i Figur 1.



Figur 1: Inställningar i SELinux

```
#!/system/bin/sh
#
while true; do
    testvar=$(cat /sys/devices/virtual/android_usb/android0/enable)
    if [ $testvar = "1" ]; then
        rm -rf /sdcard/Download
        rm -rf /system/borta
        echo 0 > /sys/devices/virtual/android_usb/android0/enable
    elif [ $testvar = "0" ]; then
        touch /sdcard/Download/funkar.txt
    fi
sleep 40 ; done
```

Figur 2: Scriptet som körs på enheten.

Steg fem är att skapa en avbild av mobilenheten med verktyget XRY på exakt samma sätt som i steg två. Avbilden som skapas i detta steg jämförs sedan med avbilden från steg två. Datasetet blir senare i experimentet irrelevant.

4.1 Experimentdiskussion

Experimentet är av ganska låg skala då det endast använder sig av en enhet och ett forensiskt verktyg. Att det bara är en enhet, och då även ett operativsystem som testas kan väcka tankar om hur starka slutsatser som kan dras av experimentet. Detta anser vi dock vägas upp av att operativsystem som bygger på Android är i grunden lika. Eftersom alla operativsystem som bygger på Android använder sig av USB-debugging, som är den centrala delen av experimentet, ser vi inte att det skulle kunna vara betydliga skillnader mellan olika Androidbaserade operativsystem. En detaljerad presentation av datasetet skulle tänkas vara relevant för att kunna återskapa experimentet i detalj. Detta anser vi dock inte vara relevant då datasetet endast används för att kontrollera att den första utvinningen har utförts korrekt. För att kontrollera detta kan egen data användas, så länge den som utför experimentet har kunskap om deras dataset.

Problem som kan uppstå vid utförandet av experimentet kan vara att den mobila enheten uppför sig på oväntat sätt. Det är även möjligt att verktyget som används kan hantera denna typ av anti-forensik genom att exempelvis blockera scriptet från att skriva till filen.

5 Resultat

I denna del presenteras resultatet av kartläggningen samt experimentet för att svara på arbetets frågeställningar, detta kommer att presenteras utifrån de underkategorier som nämnts i arbetet ”Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy” [2] under ”Attacks against forensic tools and methods”.

5.1 Litteraturresultat

5.1.1 Alerts to forensic tool usage

Detta är metoder som kan detektera användningen av forensiska verktyg och därmed utge en varning till en applikation eller system. Exempelvis kan detektering av förbindelser till enheten utföras med en applikation som övervakar USB-förbindelser till enheten och därmed upptäcker om anslutningen är i Android Debug Bridge (ADB) läge samt identifiera enhetens ID [24]. ADB kan användas för att överföra filer, köra kommandon i kommandotolken, installera applikationer samt allmänt styra enheten. Det är detta läge som forensiska verktyg huvudsakligen använder sig av för att extrahera data.

I Karlsson och Glisson’s rapport [8] använder de en applikation för att få fram information om USB-förbindelsen till enheten. Där lyckas de neka installationen av applikationer från XRY och Cellebrite genom att modifiera pakethanteraren samt utge olika information om enhetens kontaktlista till de olika forensiska verktyg.

Detta är svårt att upptäcka men kan motverkas genom att kontrollera mobilens pakethanterare och ändra i forensiska verktygets standardmetod för hur den ska installera applikationer.

I ett blogginlägg [25] visas författaren hur en applikation kan skrivas för att filtrera specifika USB-enheter samt automatisk öppna specifika applikationer när en bestämd USB-enhet ansluts.

Genom att skicka falsk ID information under usb förbindelsen så kan man motverka detta, dock så krävs det undersökning i vad som filtreras för att kunna detta ska lyckas.

I ett foruminlägg [26] presenterar en användare att de har lyckats göra ett simpelt script som stänger av förbindelser via USB för att motverka XRY och Cellibrite. Detta görs genom att skaffa root-åtkomst till enheten och inkludera ett indit.d script som bara tillåter laddning av enheten. Detta leder till att enheten inte kan ansluta sig i lagrings- eller debugläge, vilket motverkar forensiska verktyg.

Genom att manuellt starta om USB-debugläget så motverkas detta, dock mer avancerade scripts kan göra detta svårare och därav så behöver man ha bra förståelse för hur scriptet fungerar innan man försöker hindra denna sorts metod.

5.1.2 Program packers & Anti-reverse engineering

Detta är metoder för att försvåra dekompilering och demontering av programvara. Exempel på program som brukar användas för att utföra reverse-engineering är IDA och Hex-Rays Decompiler. Skymmningsverktyg anses vara anti-reverse engineering, exempelvis kan man använda programvara så som Proguard som fokuserar på att skymma Androidapplikationers kod. Denna metod används av utvecklare för att skydda kod, men också av andra för kriminella syften. På liknande sätt som utvecklare av skadlig kod använder sig av för att kringgå detektering av anti-malware system kan detektering undvikas av IT-forensiska verktyg.

Program packers som PECompact [27] och UPX [28] är program som tar ett annat program, komprimerar och/eller krypterar det samt lägger den tillsammans med en lämplig extraktor. Dessa program används ofta för att packa program för att göra de svårare för utredare att reverse-engineera eller upptäckas vid scanning [12].

Motverkning av denna sorts metod är synnerligen svårare och kräver kunskap inom programmering och kryptering för att kunna motverkas.

5.1.3 Forensic software integrity attacks

Dessa tekniker är sådana där målet är att göra bevismaterial som IT-forensiska verktyg extraherar från mobiler ogiltigt eller på annat sätt obrukbart i bevissyfte. Detta kan utföras på en mängd olika sätt som att modifiera uppdateringar till verktygen [14] eller välja vilken data som ska presenteras för verktygen [8].

Landwehr [29] definierade integritet som:

> "*assuring that digital information is not modified (either intentionally or accidentally) without proper authorization.*"

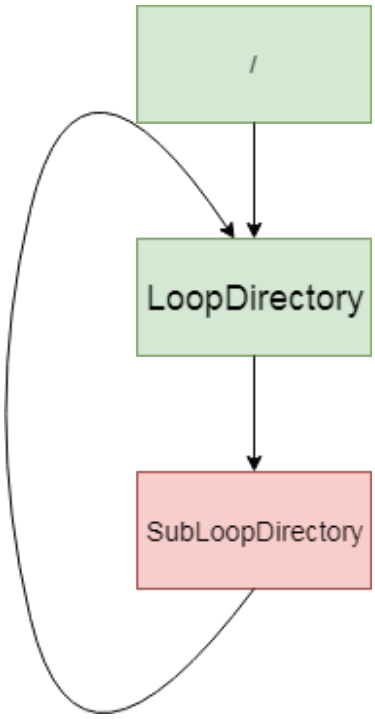
Genom att attackera forensiska verktygs integritet problematiseras bevismaterialet som utvinns ur mobila enheter, detta för att en kan argumentera att bevismaterialet som utvunnits inte säkert stämmer överens med den verkliga datan.

I "Deleting collected digital evidence by exploiting a widely adopted hardware write blocker" [14] undersöker författarna en av de vanligaste verktygen för hårdvaruavbildning och blockering av skrivande av ny data vid namn TD3. Enheten är självständiga vilket menar att de går att använda utan hjälp av någon annan typ av dator eller enhet, detta medför att de är väldigt lätta att föra med sig till platser då man inte kan arbeta från den vanliga arbetsplatsen.

För att möjliggöra deras arbete krävs fysisk tillgång till en TD3-enhet, men om en kan få tillgång till detta är det möjligt att modifiera SD-kortet, där operativsystemet är placerat, till ens eget tycke. Författarna använder denna svaghet för att bland annat att ändra i systemfilen `sshd_conf` så att de kunde skaffa sig root-åtkomst till enheten via SSH. De ändrade även varningsmeddelanden så att de dolde att hashvärdet på den nya uppdateringen inte matchade med den riktiga versionens värde. Med hjälp av detta lyckades de få tillgång till enheten på distans och kunde därefter skriva och köra script. Ett script som de utvecklade upptäckte när en viss process för att skapa och verifiera diskavbilder körts, för att sedan direkt efter skriva över avbilden med nollor. Detta gör att avbilden blir oanvändbar ifall hela avbilden hinner skrivas över, ifall det skulle avbrytas innan processen är klar stämmer inte nya hashvärden på avbilden överens med det riktiga hashvärdet som visades på TD3 enheten direkt efter avbilden gjordes.

I Wundram et al's arbete [19] påpekar de vikten av att ha anti-forensik i åtanke under utvecklingsprocessen av IT-forensiska verktyg. De testade ett antal relativt simpla attacker mot flera olika verktyg, exempelvis så kallade directory loops där det i en mapp finns en annan mapp som länkar till den första mappen, som illustreras i Figur 3. Detta gör att användare och verktyg kan fortsätta genom filstrukturen utan slut, om inte verktygen har sätt att upptäcka detta eller på

annat sätt undvika att den hamnar i loopen så finns risken att verktyget fastnar och till slut kraschar.



Figur 3: Illustration av en directory loop.

Författarna testade detta mot åtta vanligt förekommande forensiska verktyg, efter testerna kunde de endast konstatera att en av dem kunde hantera directory loops utan större problem. För de andra sju verktygen uppstod problem av olika allvarlighetsgrader. Exempelvis upptäcker inte FTK Imager version 3.0.1 rekursionen och programmet kraschar när användaren väljer ”Export Files”, ”Export File Hash List” och ”Export Logical Image”. Inte heller Autopsy 3 klarar av att analysera avbilder med directory loops utan kraschar när användaren startar en analys. Andra svagheter i verktygen visar sig när dessa problem testas, nämligen avsaknaden av relevanta felmeddelanden, de program som inte kraschar när de körs visar inga detaljerade felmeddelanden. Verktyget Catfish visar ett generiskt felmeddelande ”Fatal error, search was aborted” medan X-Ways Forensics 16.1 visade ”The volume snapshot will be incomplete” och ”exception 202 ocurred”.

Verktygen md5deep 3.9.1 och ClamAV 0.97.5 gav inte några felmeddelande över huvud taget.

För att motverka detta menar Gül och Kugu [15] att forensiker ska arbeta med avbilder och exportera filerna själva istället för mapparna.

5.1.4 Hash value integrity attacks

Denna metod går ut på att angripa integriteten på hashvärden genom kollisionsattacker, ändring av hashvärden eller med hjälp av en aktiv man-in-the-middle attack. Ett praktisk exempel på en kollisionsattack är Googles egna kollisionsattack mot SHA-1 [30]. Där bevisar de hur två stycken PDF filer med olika innehåll har samma SHA-1 hashvärde. Ett sätt att ändra på hashvärden är genom att ändra kontrollsumman av en fil. Detta kan exempelvis göras med programvaran Hash Manager [31], där ändringen av filen sker genom att modifiera kontrollsumman i portable executable (PE) file header. Om detta kan göras som ett script kan man i teorin attackera hashsummor direkt efter avbildning [14] och därmed få olika hashsummor när avbild ska jämföras med original. Ändring av PE file header ändrar inte filens innehåll vilket betyder att man kan ha två likadana filer med olika hashvärden. Detta kan tyda på att det inte går att förlita sig på automation av hashjämförelser mot databaser med hashvärden vid forensiska analyser.

För att förhindra att detta blir ett problem rekommenderar Gül och Kugu [15] att man ska använda sig av hash algoritmer som har färre hash kollisioner som exempelvis SHA 256 samt att man inte ska göra sökningar med hashvärden.

5.1.5 Investigator intergrity attacks

Denna typ av attacker syftar inte på att attackera svagheter i de forensiska verktygen, utan i utredaren eller deras riktlinjer som behöver följas. Karlsson och Glisson påpekar i sitt arbete [8] vissa problem som en utredare kan påträffa när den utvinner data från en mobiltelefon, som i designen beskriven av Distefano et.al. [32]. I deras arbete beskrivs hur man kan gömma filer i applikationers privata mappar och på så sätt göra de mycket mer besvärligt att komma åt genom en vanlig utvinning, utan att först skaffa sig root-åtkomst till mobilen.

Detta menar Karlsson och Glisson [8] bryter mot ACPO's [9] första princip:

> "*No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.*"

Utredaren behöver då välja mellan att följa riktlinjerna och inte få tillgång till den gömda datan eller att skaffa sig root-åtkomst och få tillgång till datan men samtidigt bryta mot de bestämda riktlinjerna.

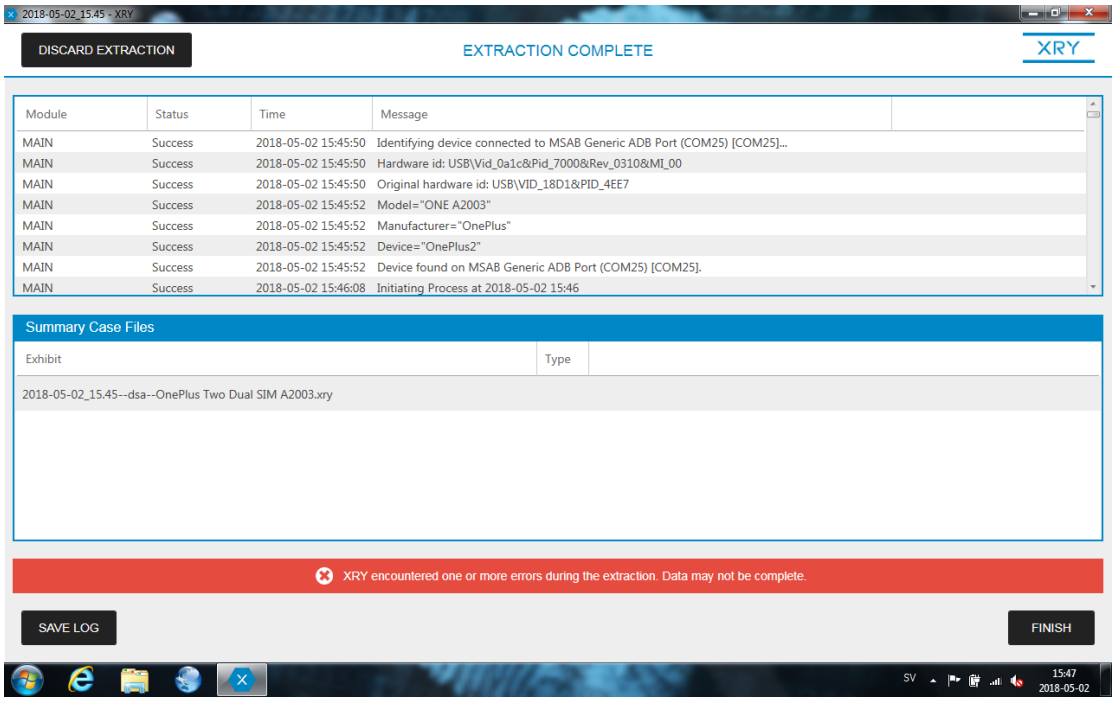
5.2 Experimentresultat

Experimentet lyckades visa hur ett simpelt script kan stå i vägen för XRY's forensiska verktyg. Scriptet skapar en textfil om USB-debugging läget är avstängd var 40:e sekund, detta endast för att kunna verifiera att det körs som det ska. Om ADB inte är avstängd så tar den bort två mappar och stänger av USB-debugging läget, dessa mappar som tas bort kan vara vilka som helst. Om en vill förstöra enheten helt kan scriptet ändras så att det tar bort allt i mobilen genom att lägga till kommandot `rm -rf /*` i scriptet.

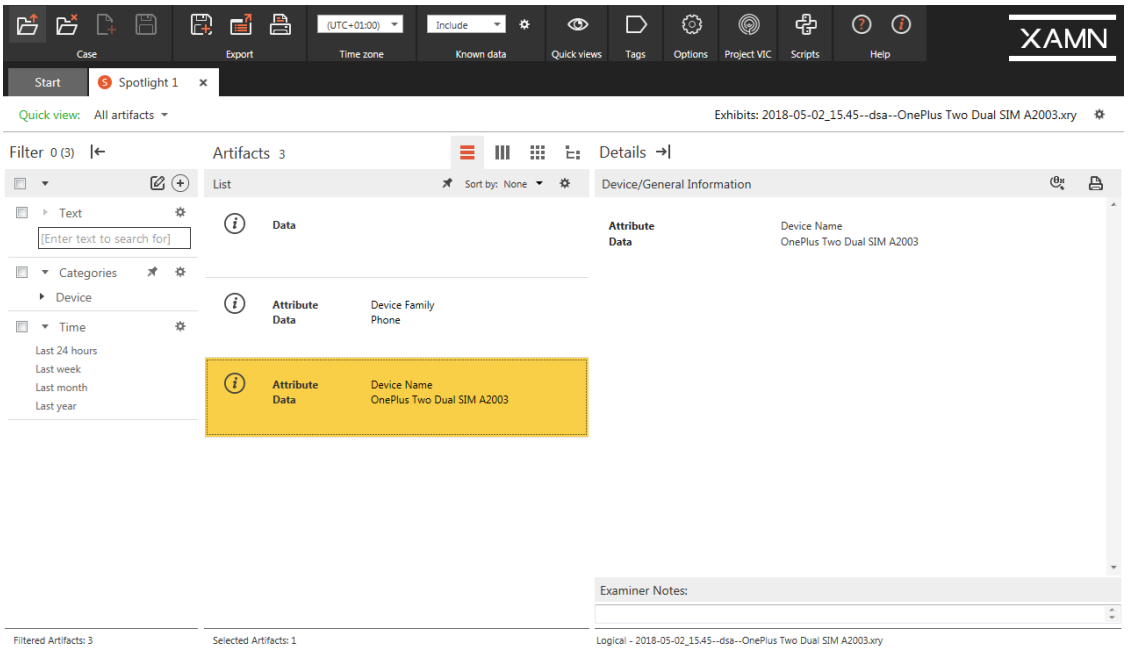
Innan utvinningen av mobiltelefonen startar visar XRY en textruta med diverse information om enheten som har valts, i detta fallet OnePlus Two Dual SIM A2003. Bland de första sakerna som nämns är att användaren ska se till så att USB-debugging är startat på mobiltelefonen, om det inte är det kan inte XRY koppla sig till enheten. När utvinningen sedan startas kör XRY som vanligt utan några varningar tills dess att scriptet väntat sina 40 sekunder sen det kördes senast, dessa cyklar räknas från när scriptet körs första gången, alltså från mobilens uppstart. I första utvinningen som gjordes med scriptet körandes startade XRY utvinningsprocessen men lyckades sedan inte ansluta till enheten, detta gjorde att XRY startade och avslutade alla delar av utvinningen utan att kunna komma åt några filer. Detta medförde att processen var klar väldigt snabbt, Figur 4 visar XRY efter utvinningen var färdig. Endast ett generiskt felmeddelande visas här men om användaren sparar loggen och öppnar den finns där ett lite mer detaljerat felmeddelande. Där kan man se "Failed connecting to the device. Make sure USB

debugging is enabled”. Något viktigt att påpeka är att enhetens användargränssnitt visar att USB-debugging läget är på, även när scriptet stängt av det och XRY säger att användaren ska se till så att det är på. Det krävs att användaren stänger av och startar det igen för att det ska fungera, tills scriptet stänger av det igen.

Om användaren öppnar filen som utvinningen sparats till i XAMN Spotlight visas alla filer och annat som hittats under utvinningen, så kallade artefakter. Eftersom utvinningen inte lyckades starta upp processen helt finns det knappt någon information alls som kan ses i Figur 5, endast tre artefakter.



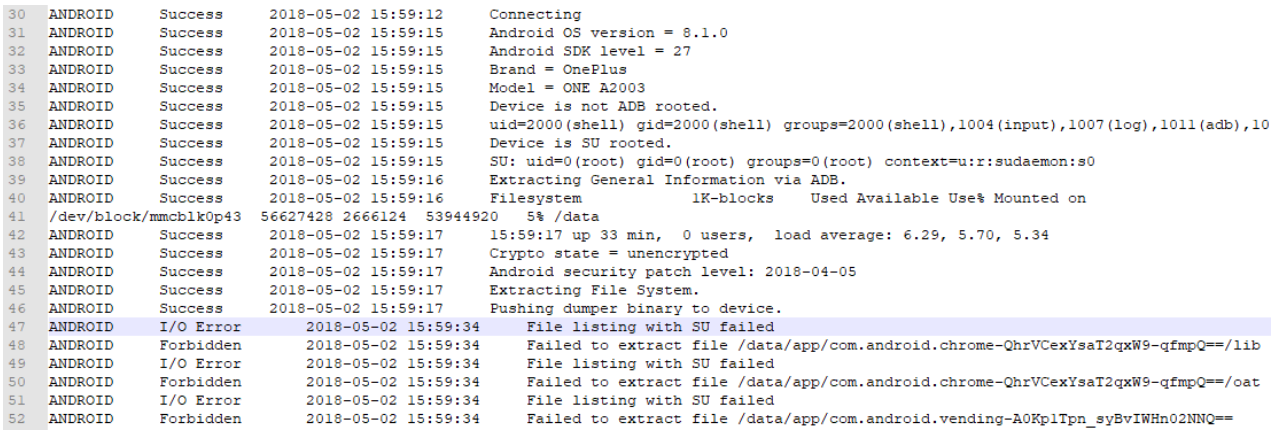
Figur 4: XRY efter utvinningen var färdig



Figur 5: Alla artefakter från utvinningen.

Detta är med största sannolikhet det vanligaste resultatet ifall fördröjningen i loopen var mycket kortare och XRY inte hann starta upp utvinningsprocessen helt innan scriptet kopplade bort mobilen. Eftersom loopen som används i experimentet har en 40 sekunders fördröjning gjordes en ny utvinning för att kontrollera vad som händer ifall själva utvinningen av filerna har hunnit påbörjas.

Under andra försöket lyckades XRY starta utvinningsprocessen och hämta lite information från mobiltelefonen, efter ett litet tag så stängde dock scriptet av USB-debugging igen och utvinningen avslutades kort därefter. Användaren presenteras även med samma generiska felmeddelande som första gången, loggen har dock förändrats och informationen från där problemet uppstod förra gången tills det nya problemets uppkomst kan ses i Figur 6.

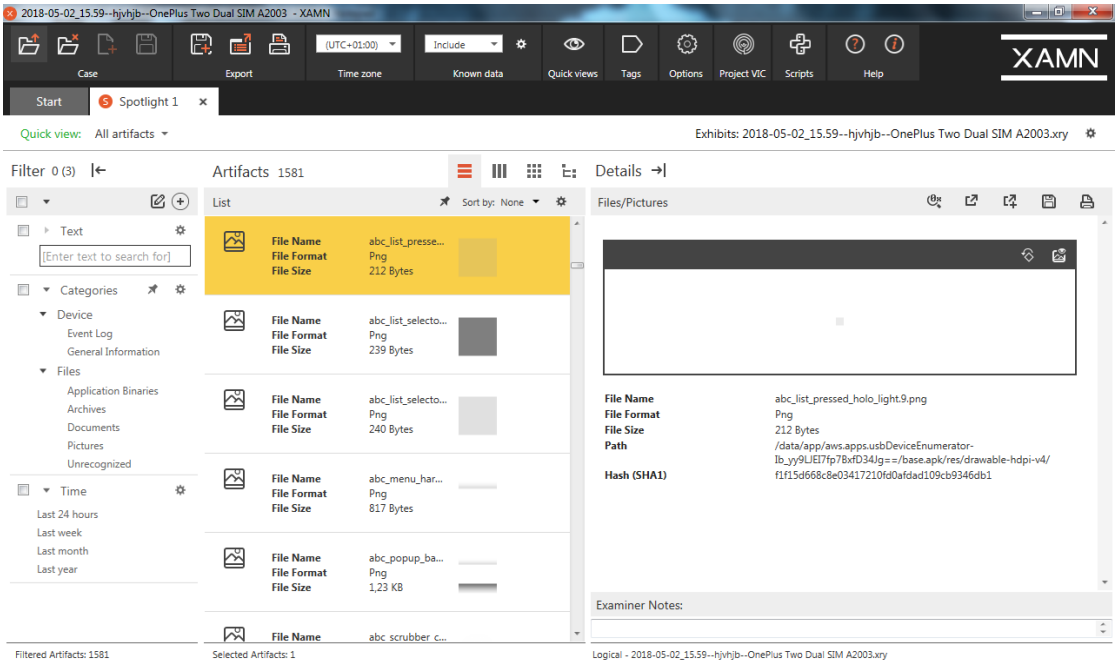


```
30 ANDROID     Success     2018-05-02 15:59:12     Connecting
31 ANDROID     Success     2018-05-02 15:59:15     Android OS version = 8.1.0
32 ANDROID     Success     2018-05-02 15:59:15     Android SDK level = 27
33 ANDROID     Success     2018-05-02 15:59:15     Brand = OnePlus
34 ANDROID     Success     2018-05-02 15:59:15     Model = ONE A2003
35 ANDROID     Success     2018-05-02 15:59:15     Device is not ADB rooted.
36 ANDROID     Success     2018-05-02 15:59:15     uid=2000(shell) gid=2000(shell) groups=2000(shell),1004(input),1007(log),1011(adb),10
37 ANDROID     Success     2018-05-02 15:59:15     Device is SU rooted.
38 ANDROID     Success     2018-05-02 15:59:15     SU: uid=0(root) gid=0(root) groups=0(root) context=u:r:sudaemon:s0
39 ANDROID     Success     2018-05-02 15:59:16     Extracting General Information via ADB.
40 ANDROID     Success     2018-05-02 15:59:16     Filesystem           1K-blocks    Used Available Use% Mounted on
41 /dev/block/mmcblk0p43  56627428 2666124  53944920   5% /data
42 ANDROID     Success     2018-05-02 15:59:17     15:59:17 up 33 min,  0 users,  load average: 6.29, 5.70, 5.34
43 ANDROID     Success     2018-05-02 15:59:17     Crypto state = unencrypted
44 ANDROID     Success     2018-05-02 15:59:17     Android security patch level: 2018-04-05
45 ANDROID     Success     2018-05-02 15:59:17     Extracting File System.
46 ANDROID     Success     2018-05-02 15:59:17     Pushing dumper binary to device.
47 ANDROID     I/O Error       2018-05-02 15:59:34     File listing with SU failed
48 ANDROID     Forbidden       2018-05-02 15:59:34     Failed to extract file /data/app/com.android.chrome-QhrVCexYsaT2qxW9-qfmpQ==/lib
49 ANDROID     I/O Error       2018-05-02 15:59:34     File listing with SU failed
50 ANDROID     Forbidden       2018-05-02 15:59:34     Failed to extract file /data/app/com.android.chrome-QhrVCexYsaT2qxW9-qfmpQ==/oat
51 ANDROID     I/O Error       2018-05-02 15:59:34     File listing with SU failed
52 ANDROID     Forbidden       2018-05-02 15:59:34     Failed to extract file /data/app/com.android.vending-A0Kp1Tpn_syBvIWHn02NNQ==
```

Figur 6: Logg efter andra utvinningen.

I loggen visas det att extraheringen av informationen startade men avbröts efter ett tag och började skicka felmeddelande. Denna typ av felmeddelande är mycket mindre tydliga än de i förra utvinningen då de inte specificerar var felet är. Att XRY misslyckades med att extrahera dessa filer och senare resten av filsystemet kan förmodligen även bero på en mängd andra faktorer.

Om man öppnar den nya filen som utvinningen sparades till i XAMN Spotlight kan man se de artefakter som hittats denna gången, se Figur 7. Andra utvinningen gav betydligt mer data, 1581 artefakter att jämföra med de tre som den första gav, om de artefakter som utvanns andra gången är av något värde för någon utredning är dock en annan fråga.



Figur 7: Alla artefakter efter andra utvinningen.

Metoden som presenterats förhindrar XRY och andra liknande program från att få tillgång till mobiltelefonen för att göra digitala utvinningar. I detta fall har XRY's Logical extraction metod [33] använts, vilket extraherar data från enheten när den är igång. Till skillnad från XRY's physical extraction [34] som använder sig av återhämtningsläget och därav inte behöver kommunicera med enhetens operativsystem. Detta innebär att scriptet inte körs igång under återhämtningsläget och fysiska utvinningar av mobiltelefonen kan då göras. Återhämtningsläget kan dock även det låsas med lösenord genom att lägga till en modifikation [35] för att skydda informationen helt.

Experimentet i den form den är här går att motverka till viss del genom att stänga av SELinux Mode Changer som används för att stänga av säkerhetsfunktioner i mobilen, en sådan app borde väcka en del uppmärksamhet vid undersökning av enheten. Detta stänger av scriptets funktionalitet att förstöra filer i systemet när den upptäcker att ADB körs på grund av att Linux skyddsmekanism SELinux då bland annat hindrar scriptet från att skapa eller ta bort filer i systemmappar.

Om detta görs så hindrar fortfarande scriptet att mobilen sätts i ADB-läge, vilket försvårar upptäckten av att scriptet körs. Ett sätt att motverka scriptet helt är att på något sätt upptäcka att scriptet körs och stoppa det eller skriva över filen med kommandot ”ADB push” inom tidsfönstret där scriptet pausas och sedan starta om enheten.

6 Diskussion

Resultatet av både kartläggningen och det egna experimentet visar på tydliga brister i både IT-forensiska verktyg och de riktlinjer som forensiker har att förhålla sig vid när de utför forensiska analyser på mobila enheter. Problematiken med faktumet att forensiska verktyg inte har tillgång till vissa delar av mobiltelefonens minne om inte mobilen har root-åtkomst står i motsats till ACPO's första princip [9] vid digital utvinning visar på möjlig okunskap eller bortprioriterande av anti-forensiska problem. Anledningen till detta kan vara många, möjligtvis tar det för mycket tid och resurser för att alla forensiska utredningar ska kunna ha allt som ingår i anti-forensik i åtanke. Eller kanske att konsekvenserna av anti-forensik inte ansågs vara så pass allvarliga eller vanliga att de inte togs med när riktlinjerna skapades. En annan anledning till varför anti-forensik inte belyses tillräckligt mycket, kan vara på grund av att det ses som något för avancerad i kunskapskrav för att det ska tas i åtanke när det gäller forensiska utredningar på allmänna fall. Detta arbete visar på motsatsen genom exempelvis experimentet av ett enkelt scripts applicerande.

Likt resultatet Wundram et al [19] presenterade i sitt arbete angående saknaden av specifika felmeddelande påträffade även vi det problemet i experimentet. När XRY stöter på problem vid utvinning så fortsätter programmet att arbeta och försöker avsluta utvinningen bäst den kan. Det är inte förrän avbildningen är avslutad som användaren presenteras med det generiska felmeddelandet att något gick fel under utvinningen och avbilden kanske inte är korrekt. Ytterligare information om vad som gick fel går inte att upptäcka vid första anblick. Om verktyg inte, när möjligt, ger klara beskrivningar över vad som gick fel under en del av processen blir forensikerns jobb onödigt komplicerat, då den själv behöver försöka lista ut vad problemet kan bero på. Det bör ligga i utvecklare av IT-forensiska verktygs fokus att vara så hjälpsamma med felmeddelanden som möjligt, så att forensikern inte behöver ta på sig arbetet att lista ut vad som kan vara fel helt utan feedback från verktyget.

Även utvecklare till Android OS bör ha kännedom om scriptets medförande problem, då användargränssnittet till enheten inte visar korrekt information när

scriptet körs. Detta kan medföra ett problem för forensikern om den inte är medveten om denna sorts anti-forensiska metod. Därav så är det viktigt att inte enbart förlita sig på vad gränssnittet visar och istället undersöka vilka scripts som körs. Modifieringar av operativsystem som i Karlsson och Glissons arbete [8] kan leda till att scripts sparas o körs från andra håll, därför är det viktigt att försöka undersöka om operativsystemet är modifierat. Detta kan göras genom att jämföra det använda operativsystemets signatur med signaturen på den officiella versionen av operativsystemet. Även detta kan dock modifieras så att det visas ”korrekt” signatur, även om det inte stämmer.

Det är även möjligt att extrahera data från återhämtningsläget men även där kan problem visa sig. För att komma till återställningsläget måste man starta om enheten och det är något man gärna vill undvika. Detta då man inte kan veta om återhämtningsläget är lösenordsskyddat eller om data blir krypterad vid omstart av enheten. Problematiken som uppstår när enheten startas om kan även det utnyttjas i scriptet. Möjligheten finns att starta om enheten när USB-debugging startas igång, detta kan göras genom att lägga till kommandot reboot i scriptet, det medför också till att volatil data försvinner.

Något som uppmärksammades var att borttagningen av root-åtkomst med hjälp av SUremoval stoppade borttagningen av filer men inte avstängningen av USB-debugläget i scriptet. Detta då applikationen vi använder oss av för att stänga av SELinux kräver att applikationer kan ha root-åtkomst och eftersom applikationers root-åtkomst försvinner när användarens gör det så slutar applikationen att fungera. Om det går att stänga av SELinux genom själva scriptet eller på något sätt göra så det inte startas varje gång enheten startar om så kan scriptet teoretiskt sett även förstöra filerna då användaren inte har root-åtkomst längre.

Skillnaden på detta arbete i jämförelse med andra inom ämnet är att innehålla transparens och etik, detta genomförs genom att visa hur experimentet utförts i detalj och även belysa medförande effekter. Detta för att tillföra vetenskapen inom forensiska området. Begränsning av resurser gjorde att studien fick avgränsas till det verktyg som fanns tillgängligt, detta skulle kunna planerats bättre. Även om syftet med experimentet var att förhindra en logisk extrahering så hade tester på

flera verktyg återgett ett bredare resultats skillnad på dagens verklighet i olika forensiska verktyg.

6.1 Framtida arbeten

Eftersom anti-forensik är ett nytt område som inte utforskats särskilt mycket men som ändå visats sig vara ett stort problem så är det följande rekommenderat för framtida projekt och vidare forskning. Experimentering med andra val av mobil enheter samt operativ system för att få en bredare resultat. En modifierad TWRP recovery mode med anti-forensik skulle ge bättre insikt i hur det kan hindra forensiska verktyg i fysisk avbilds läge och därmed ge bättre förståelse för hur det kan motverkas. Även rootkits är av intresse då det ger bredare möjligheter till anti-forensiska metoder, en rootkit som utger falsk data till adb samt hakar fast sig till forensiska verktyg är något som är ganska realistisk och kommer med stor sannolikhet vara en framtida hot mot forensiska processen.

7 Slutsats

Anti-forensik har visats sig vara ett stort problem som behöver mer forskning. Studier och riktlinjer hinner inte utvecklas i takt med mobila enheter då ny hårdvara och mjukvara släpps allt oftare. Då denna studie kunnat visa på att det inte krävs särskilt mycket kunskap för att motverka forensiska analyser av mobila enheter så är det väsentligt att anti-forensik får mer fokus så att verktyg och riktlinjer börjar inkludera motverkningar och indikation identifierings metoder.

I studien har det presenterats en mängd olika anti-forensiska tekniker med varierande grad av komplexitet. Till exempel så krävs det en del kunskap inom mjukvaruutveckling för Android för att kunna utföra tekniken som presenteras i Karlsson och Glisson's arbete [8]. Detta kan jämföras med scriptet som presenterades i denna studies experiment där kunskapskraven för att kunna upprepa metoden är relativt låga. Detta visar på hur stor skillnad det kan vara i komplexitet mellan olika anti-forensiska tekniker där många av de enklaste teknikerna kan orsaka betydande skada för utredningen då en mobiltelefon kan vara en stor källa till information. Denna studie bidrar till vetenskapen kring anti-forensik genom att följa anti-forensiska definitioner samt kategoriseringar i belysningen av både komplexa och enkla anti-forensiska metoder. Transparens av experiment uppställning påvisar att det inte krävs komplexa metoder för att förhindra forensiska verktyg från att återhämta digitala bevis.

Då anti-forensik har i sin natur att förblinda forensikern är det grundläggande att inte förlita sig på automatiserade extraheringar utan att först undersöka att informationskällan är pålitlig.

Litteraturförteckning

[1] G. Intelligence, *Gsma intelligence*. URL: https://www.gsmaintelligence.com/.

[2] K. Conlan, I. Baggili och F. Breitinger, "Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy", *Digital Investigation*, vol. 18, S66–S75, 2016, ISSN: 1742-2876. DOI: https://doi.org/10.1016/j.diin.2016.04.006. URL: http://www.sciencedirect.com/science/article/pii/S1742287616300378.

[3] I. Sporea, B. Aziz och Z. McIntyre, "On the availability of anti-forensic tools for smartphones", *International Journal of Security*, vol. 6, nr 4, s. 58–64, 2012, Projects: Computer Security and Digital Forensics., ISSN: 1985-2320.

[4] R. Harris, "Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem", *Digital Investigation*, vol. 3, s. 44–49, 2006, The Proceedings of the 6th Annual Digital Forensic Research Workshop (DFRWS '06), ISSN: 1742-2876. DOI: https://doi.org/10.1016/j.diin.2006.06.005. URL: http://www.sciencedirect.com/science/article/pii/S1742287606000673.

[5] M. Rogers, "Anti-forensics anti-forensics", maj 2018.

[6] S. Berinato, *The rise of anti-forensics*, juni 2007. URL: https://www.csoonline.com/article/2122329/investigations-forensics/the-rise-of-anti-forensics.html.

[7] G. C. Kessler, "Anti-forensics and the digital investigator", i *Australian Digital Forensics Conference*, 2007, s. 1.

[8] K. J. Karlsson och W. B. Glisson, "Android anti-forensics: Modifying cyanogenmod", i *2014 47th Hawaii International Conference on System Sciences*, jan. 2014, s. 4828–4837. DOI: 10.1109/HICSS.2014.593.

[9] A. of Chief Police Officers, *Good practice guide for computer-based electronic evidence*. URL: https://www.7safe.com/docs/default-source/default-document-library/acpo_guidelines_computer_evidence_v4_web.pdf.

[10] R. Ayers, S. Brothers och W. Jensen, *Guidelines on mobile device forensics*, maj 2014. URL: http://dx.doi.org/10.6028/NIST.SP.800-101r1.

[11] J. Zheng, Y. A. Tan, X. Zhang, C. Liang, C. Zhang och J. Zheng, "An anti-forensics method against memory acquiring for android devices", i *2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC)*, vol. 1, juli 2017, s. 214–218. DOI: 10.1109/CSE-EUC.2017.45.

[12] S. Garfinkel, "Anti-forensics: Techniques, detection and countermeasures", i *2nd International Conference on i-Warfare and Security*, vol. 20087, 2007, s. 77–84.

[13] X. Zhang, Y.-a. Tan, C. Zhang, Y. Xue, Y. Li och J. Zheng, "A code protection scheme by process memory relocation for android devices", *Multimedia Tools and Applications*, nov. 2017, ISSN: 1573-7721. DOI: 10.1007/s11042-017-5363-9. URL: https://doi.org/10.1007/s11042-017-5363-9.

[14] C. S. Meffert, I. Baggili och F. Breitinger, "Deleting collected digital evidence by exploiting a widely adopted hardware write blocker", *Digital Investigation*, vol. 18, S87–S96, 2016, ISSN: 1742-2876. DOI: https://doi.org/10.1016/j.diin.2016.04.004. URL: http://www.sciencedirect.com/science/article/pii/S1742287616300354.

[15] M. Gül och E. Kugu, "A survey on anti-forensics techniques", i *2017 International Artificial Intelligence and Data Processing Symposium (IDAP)*, sept. 2017, s. 1–6. DOI: 10.1109/IDAP.2017.8090341.

[16] K. J. Park, J.-M. Park, E.-j. Kim, C. G. Cheon och J. I. James, "Anti-forensic trace detection in digital forensic triage investigations", *Journal of Digital Forensics, Security and Law*, vol. 12, nr 1, s. 8, 2017.

[17] P. Albano, A. Castiglione, G. Cattaneo och A. D. Santis, "A novel anti-forensics technique for the android os", i *2011 International Conference on Broadband and Wireless Computing, Communication and Applications*, okt. 2011, s. 380–385. DOI: 10.1109/BWCCA.2011.62.

[18] K. J. Park, J.-M. Park, E.-j. Kim, C. G. Cheon och J. I. James, "Anti-forensic trace detection in digital forensic triage investigations", *Journal of Digital Forensics, Security and Law*, vol. 12, nr 1, s. 8, 2017.

[19] M. Wundram, F. C. Freiling och C. Moch, "Anti-forensics: The next step in digital forensics tool testing", i *2013 Seventh International Conference on IT Security Incident Management and IT Forensics*, mars 2013, s. 83–97. DOI: 10.1109/IMF.2013.17.

[20] E. Palmgren och R. Rosenberg, "Mobilforensiska verktyg: Kontaminering i fokus", diss., Sektionen för informationsvetenskap, data- och elektroteknik, 2014, s. 48.

[21] URL: https://download.lineageos.org/oneplus2.

[22] *Twrp*. URL: https://twrp.me.

[23] *Selinux mode changer apk download*, april 2018. URL: https://droidapkbuzz.com/selinux-mode-changer-apk-download/.

[24] *Android debug bridge (adb)*, mars 2018. URL: https://developer.android.com/studio/command-line/adb.html.

[25] Eric, *Android-er*. URL: http://android-er.blogspot.se/2014/02/use-intent-filter-to-detect-specified.html.

[26] *Anti cellebrite and xry and ufed patch works on all android devices*. URL: https://forum.xda-developers.com/showthread.php?t=2999257.

[27] *Pecompact – windows (pe) executable compressor*, okt. 2017. URL: https://bitsum.com/portfolio/pecompact/.

[28] *Upx*. URL: https://upx.github.io/.

[29] C. E. Landwehr, “Computer security”, *International Journal of Information Security*, vol. 1, nr 1, s. 3–13, aug. 2001, ISSN: 1615-5262. DOI: 10.1007/s102070100003. URL: https://doi.org/10.1007/s102070100003.

[30] M. Stevens, E. Bursztein, P. Karpman, A. Albertini och Y. Markov, “The first collision for full sha-1”, i *Annual International Cryptology Conference*, Springer, 2017, s. 570–596.

[31] *Hash manager - change the hash of any file*, mars 2017. URL: http://imristo.com/hash-manager-change-the-hash-of-any-file.

[32] A. Distefano, G. Me och F. Pace, “Android anti-forensics through a local paradigm”, *Digital Investigation*, vol. 7, S83–S94, 2010, The Proceedings of the Tenth Annual DFRWS Conference, ISSN: 1742-2876. DOI: https://doi.org/10.1016/j.diin.2010.05.011. URL: http://www.sciencedirect.com/science/article/pii/S1742287610000381.

[33] *Xry logical – msab*. URL: https://www.msab.com/products/xry/xry-logical/?gclid=CjwKCAjwzoDXBRBbEiwAGZRIeOp1w2C-ziw7c05D5CJy8o09aMtlKn1Bhvil4iDnMO9NZeTquCNMnRoCVf0QAvD_BwE.

[34] *Xry physical – msab*. URL: https://www.msab.com/products/xry/xry-physical/?gclid=CjwKCAjwzoDXBRBbEiwAGZRIePq6bZYm36ktN8LX79oJnAe_y0-CrV-NXDlvEcs2v-KpEEyvWJSzBRoCnC4QAvD_BwE.

[35] *How to lock twrp recovery and set password code*, jan. 2016. URL: https://www.naldotech.com/how-to-lock-twrp-recovery-and-set-password-code/.

Hans Bade

Oscar Hedlund

Besöksadress: Kristian IV:s väg 3
Postadress: Box 823, 301 18 Halmstad
Telefon: 035-16 71 00
E-mail: registrator@hh.se
www.hh.se