Forenzika nasilnog ekstremizma u digitalnom okruženju

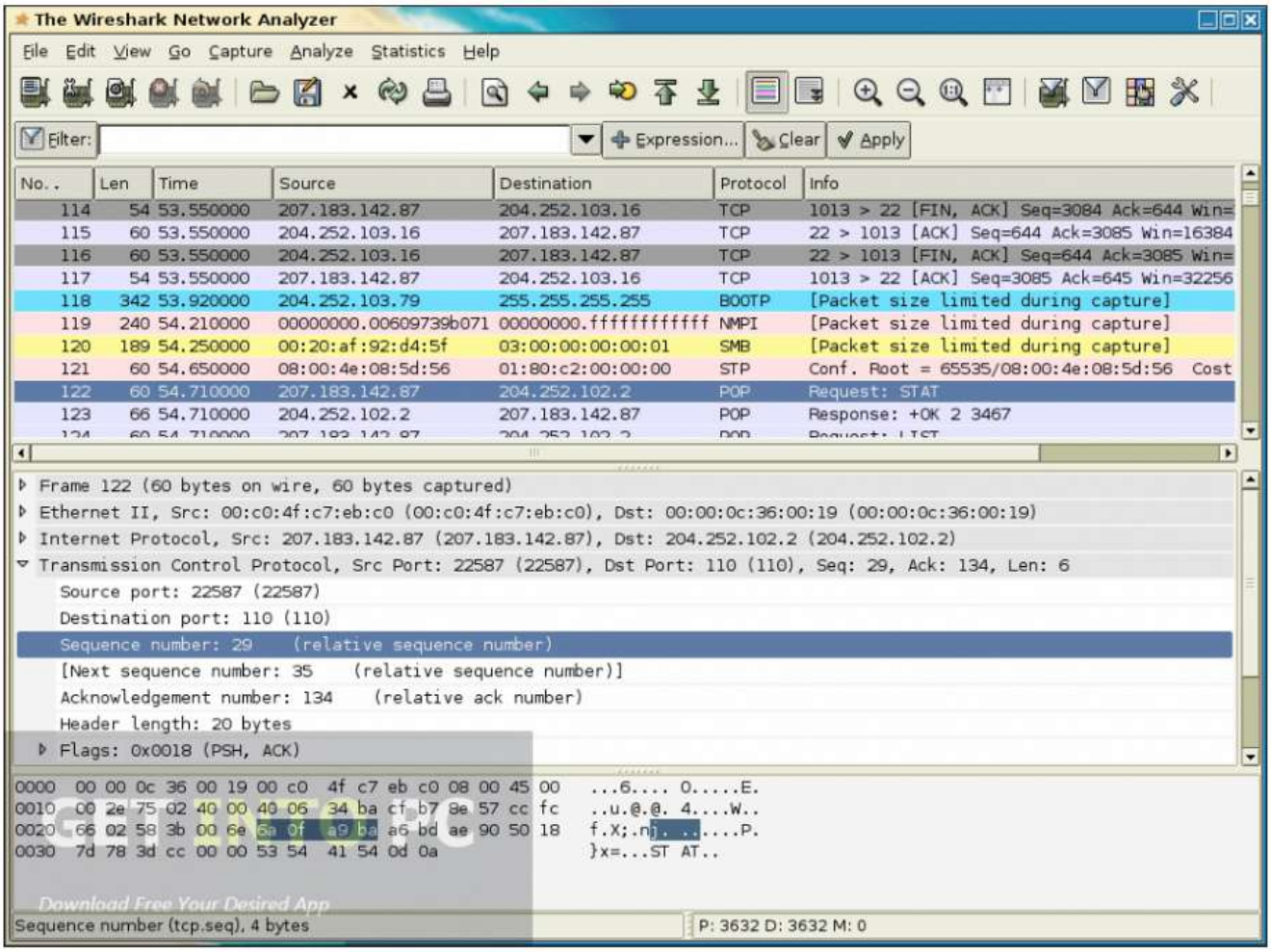
Digitalni forenzički alati

Norway
SMART Balkans
CPCD
IDM
CRPM

Forenzika nasilnog ekstremizma u digitalnom okruženju

WireShark

1



Wireshark je popularan digitalni forenzički alat i mrežni analizator koji omogućava prikupljanje i pregled mrežnog saobraćaja u realnom vremenu, kao i analizu sačuvanih mrežnih podataka. Njegova primjena je široka, a najčešće se koristi u sljedeće svrhe:

1. **Analiza mrežnog saobraćaja**: Wireshark omogućava detaljan pregled mrežnog prometa na različitim protokolima (npr. HTTP, TCP, UDP). Pomaže u identifikaciji problema sa mrežom, sporim konekcijama, gubicima paketa ili problemima u aplikacijama.

2. **Digitalna forenzika**: Kao alat za digitalnu forenziku, koristi se za identifikaciju i rekonstrukciju događaja u vezi sa potencijalnim sigurnosnim incidentima. To uključuje identifikaciju napada, upada i sumnjivog ponašanja na mreži.

3. **Otkrivanje prijetnji i otklanjanje problema u vezi sa cyber sigurnošću**: Wireshark omogućava identifikaciju zlonamjernih aktivnosti, kao što su DDoS napadi, skeniranje portova, brute-force napadi i mnoge druge vrste mrežnih napada.

4. Učenje o mrežnim protokolima: Zahvaljujući svojoj sposobnosti za prikazivanje protokola i dekodiranje mrežnog prometa, Wireshark je koristan alat za obrazovne svrhe. Koriste ga studenti, istraživači i profesionalci koji žele da bolje razumiju kako funkcionišu različiti mrežni protokoli.

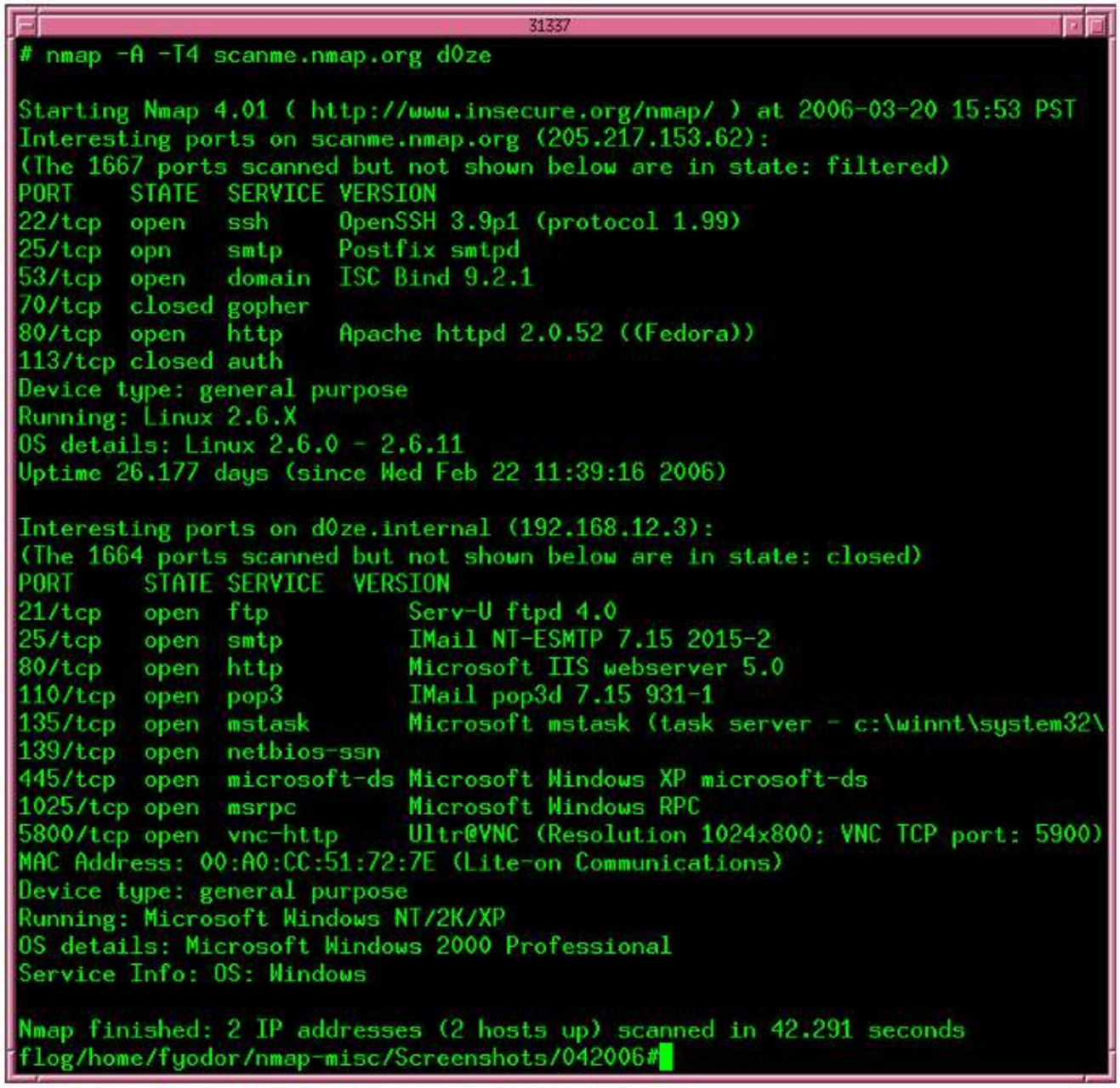
5. Dijagnostika aplikacija i optimizacija performansi: Programeri koriste Wireshark kako bi otkrili gdje dolazi do zastoja ili uskih grla u performansama mrežnih aplikacija i unaprijedili brzinu ili stabilnost aplikacija.

Wireshark je slobodan alat, dostupan za različite operativne sisteme i veoma je koristan za IT stručnjake u oblastima mrežne administracije, cyber sigurnosti i digitalne forenzike

Forenzika nasilnog ekstremizma u digitalnom okruženju

NMAP

2



Nmap (Network Mapper) je moćan alat koji se koristi za mrežno skeniranje i analizu, a često se koristi i u digitalnoj forenzici i cyber sigurnosti. Njegova osnovna funkcija je identifikacija mrežnih uređaja i njihovih karakteristika, što je ključna informacija u brojnim slučajevima digitalne istrage i mrežnih analiza. Evo glavnih primjena Nmap-a kao forenzičkog alata:

1. **Skeniranje i mapiranje mreže**: Nmap može brzo otkriti aktivne uređaje na mreži i prikazati njihovu IP adresu, otvorene portove, aktivne servise i operativni sistem. Ova funkcija je izuzetno korisna za forenzičke analitičare jer omogućava brz pregled mrežnog okruženja i identifikaciju svih uređaja u mreži.

2. Identifikacija otvorenih portova i servisa: Nmap skenira portove uređaja i identifikuje aktivne servise, što je od velikog značaja u forenzičkoj istrazi kada je potrebno utvrditi koji su servisi aktivni i koji portovi mogu biti ranjivi na napade. Na primjer, ovo može pomoći u otkrivanju neovlaštenih servisa ili portova koje koriste napadači.

3. Praćenje promjena u mrežnom okruženju: Redovnim skeniranjem mreže, Nmap omogućava otkrivanje bilo kakvih promjena, kao što su novi uređaji ili otvoreni portovi. To može signalizirati potencijalni sigurnosni problem ili napad, što je korisno u forenzičkoj istrazi.

4. Otkrivanje ranjivosti: Nmap-ovi skriptni dodaci (Nmap Scripting Engine–NSE) omogućavaju specifične pretrage i ranjivosti za određene mrežne servise. Ovo je korisno za identifikaciju poznatih ranjivosti i procjenu sigurnosnog stanja mreže.

5. Proaktivno testiranje mrežne sigurnosti: Iako Nmap nije primarno forenzički alat, može se koristiti za provjeru sigurnosti mreže i identifikaciju mogućih slabih tačaka. Ova proaktivna analiza može biti deo šire forenzičke strategije za otkrivanje potencijalnih prijetnji i zaštitu od incidenata.

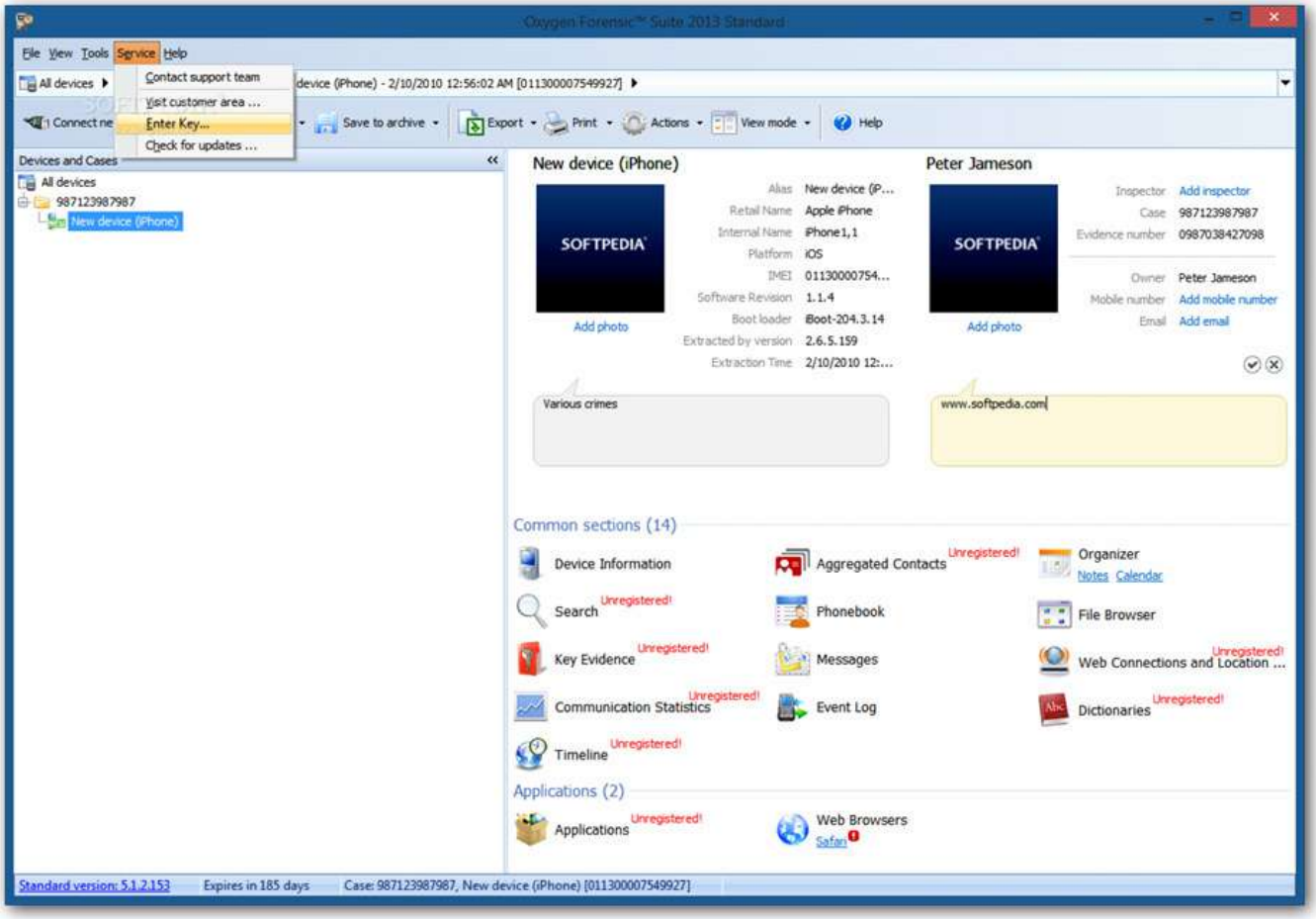
6. Otkrivanje prisustva prikrivenih uređaja: Nmap može otkriti uređaje koji koriste metode prikrivanja, poput NAT-a ili VPN-ova, što pomaže u otkrivanju naprednih prijetnji ili zlonamjernih uređaja u mreži.

Nmap je besplatan i otvorenog koda, čime je dostupan svim stručnjacima za mrežnu sigurnost i digitalnu forenziku, a koristi se u širokom spektru mrežnih analiza, od jednostavnog mapiranja mreže do složenih sigurnosnih i forenzičkih istraživanja.

Forenzika nasilnog ekstremizma u digitalnom okruženju

Oxygen forensic suite

3



Oxygen Forensic Suite je napredan forenzički softver specijalizovan za prikupljanje, analizu i izvlačenje podataka sa mobilnih uređaja, uključujući pametne telefone, tablete, cloud servise i IoT uređaje. Koristi se uglavnom u digitalnim forenzičkim istragama za dobijanje informacija koje su relevantne za istrage kriminalnih slučajeva, bezbjedonosne provjere i zaštitu podataka. Evo glavnih primjena i funkcionalnosti Oxygen Forensic Suite alata:

1. **Ekstrakcija podataka sa mobilnih uređaja**: Oxygen Forensic Suite omogućava dubinsku ekstrakciju podataka sa uređaja na različitim operativnim sistemima (Android, iOS, Windows Mobile). Može izvući podatke kao što su SMS poruke, pozivi, kontakti, kalendari, aplikacije, i GPS podaci, što je ključno u istragama gdje se traže komunikacijski dokazi.

2. **Analiza društvenih mreža i aplikacija za razmenu poruka**: Alat ima podršku za više od 400 aplikacija za razmjenu poruka i društvenih mreža (kao što su WhatsApp, Facebook, Instagram, Viber), omogućavajući analitičarima pristup podacima kao što su poruke, prilozi, multimedijalni sadržaj, historija pretrage, itd.

3. Cloud forenzika: Oxygen Forensic Suite može pristupiti podacima iz različitih cloud servisa (kao što su Google, Apple, Microsoft, Amazon) koristeći kredencijale ili identifikacione podatke sa mobilnog uređaja. Ovo omogućava istražiteljima pristup dodatnim informacijama, kao što su bekap podaci, sinkronizovani kontakti, fotografije, dokumenti i GPS historija.

4. Geolokacijska analiza: Alat pruža detaljnu analizu podataka o lokaciji na osnovu GPS koordinata, Wi-Fi konekcija, i podataka sa aplikacija kao što su Google Maps i drugi servisi za navigaciju. Ova funkcionalnost je korisna za rekonstrukciju kretanja subjekta i njegovih aktivnosti.

5. Dekripcija podataka i šifriranih aplikacija: Oxygen Forensic Suite dolazi sa ugrađenim alatima za dekripciju koji mogu pomoći u otključavanju šifriranih aplikacija i sadržaja. Ovo uključuje mogućnost rada sa enkriptovanim fajlovima i nalazima, čime se omogućava pristup zaštićenim podacima za dalju analizu.

6. Analiza IoT uređaja i pametnih nosivih uređaja: Osim mobilnih uređaja, ovaj alat može prikupiti podatke sa IoT uređaja, kao što su pametni satovi i nosiva tehnologija. Podaci sa ovih uređaja često sadrže vrijedne informacije o kretanju, zdravlju i aktivnosti korisnika.

7. Pregled i analiza mrežne aktivnosti: Alat može pružiti uvid u mrežnu aktivnost uređaja, uključujući Wi-Fi mreže na koje se uređaj povezivao, vremenske oznake i trajanje konekcija. Ova analiza može otkriti podatke o vremenu i mjestu aktivnosti uređaja.

8. Izrada izveštaja za pravne svrhe: Oxygen Forensic Suite nudi mogućnost izrade detaljnih izveštaja sa svim prikupljenim podacima, što je ključno za forenzičke analize koje će se koristiti u sudskim procesima. Izveštaji su prilagođeni i organizovani kako bi se obezbijedila jasna i pregledna prezentacija dokaza.

Oxygen Forensic Suite je često alat izbora za digitalne forenzičke analitičare i istražitelje u sektorima bezbjednosti, policije, i privatnim forenzičkim firmama zbog svoje sposobnosti da dubinski pristupi velikom broju različitih izvora podataka sa mobilnih IoT uređaja, cloud-a i aplikacija.

Forenzika nasilnog ekstremizma u digitalnom okruženju

The Sleuth kit

4

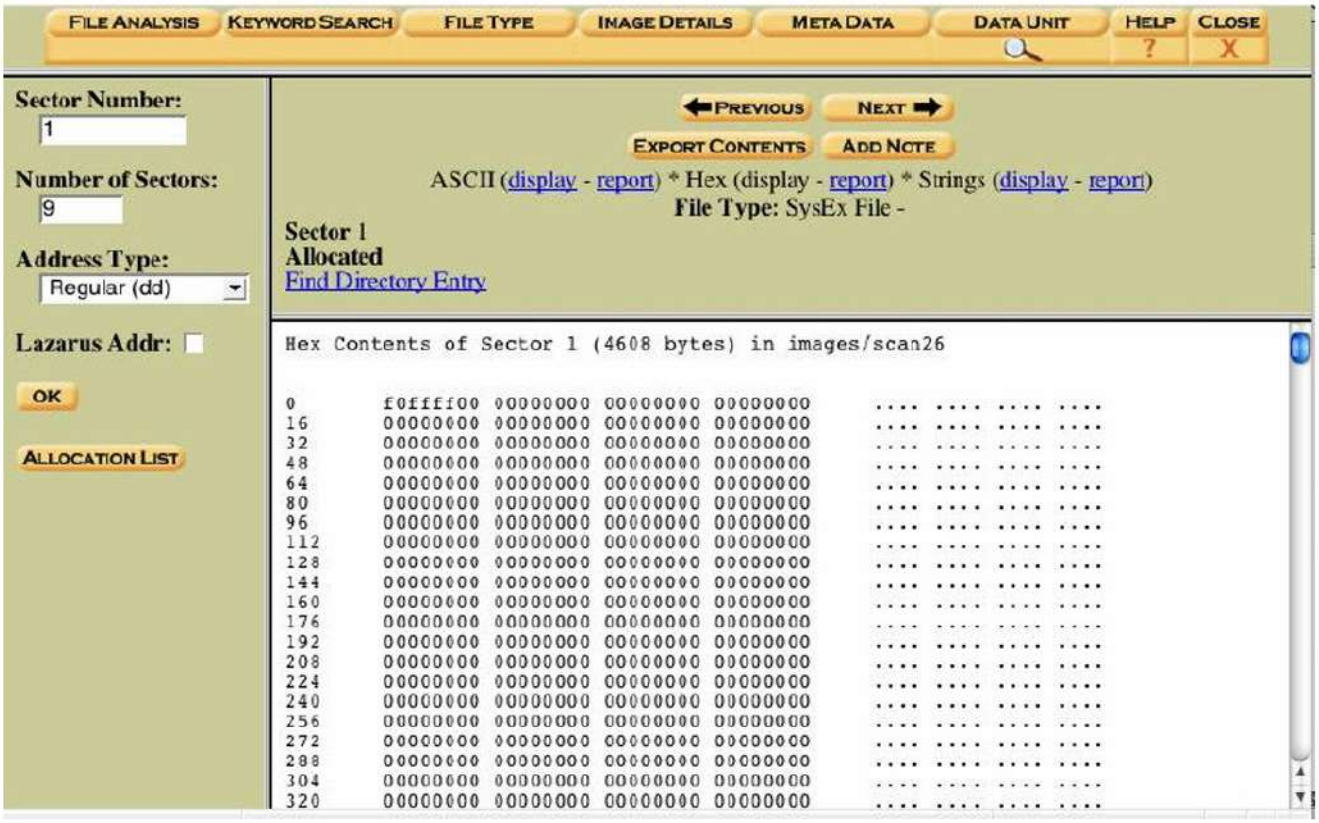
Norway

SMART Balkans
Civil Society for Shared Society in the Western Balkans

CPCD
Centar za promociju civilnog društva

IDM
Institute for Democracy and Mediation

CRPM
Center for Research and Policy Making
... policy impact since 2004



The Sleuth Kit (TSK) je besplatan i open-source alat za digitalnu forenziku, prvenstveno namenjen analizi digitalnih medija, poput tvrdih diskova i drugih skladišnih uređaja. Koristi se u istragama za rekonstrukciju i analizu datotečnih sistema, pronalaženje obrisanih datoteka, i identifikaciju zlonamernih aktivnosti na uređajima. Njegove ključne primjene uključuju sledeće:

1. Analiza datotečnih sistema: TSK podržava analizu različitih datotečnih sistema, uključujući NTFS, FAT, HFS+, Ext2/3/4, i druge. Omogućava istražiteljima pristup i pregled datoteka, direktorijuma, i metapodataka, čak i kada su podaci oštećeni ili izbrisani.

2. Ekstrakcija obrisanih podataka: TSK može identifikovati obrisane fajlove i pokušati da ih povrati. Ovo uključuje rekonstrukciju podataka iz datotečnih struktura i povrat podataka sa sektora diska, što može otkriti tragove podataka koji su namerno uklonjeni.

3. Forenzička analiza slika diska: Alat podržava rad sa forenzičkim slikama diska (kao što su E01, AFF, DD) i omogućava istražiteljima da pregledaju strukturu diska kao cjelinu bez promjene originalnih podataka. Ovo je važno za očuvanje integriteta dokaza tokom istrage.

4. Istraživanje vremenskih oznaka (timestamp analiza): TSK pruža pristup vremenskim oznakama (kao što su vrijeme kreiranja, modifikacije i pristupa datotekama), što omogućava istražiteljima da rekonstruišu redoslijed događaja. Ovo je ključno za utvrđivanje vremenskih tačaka aktivnosti na uređaju.

5. Automatizovano pretraživanje i analitika: Uz TSK dolazi niz alata i skripti koje omogućavaju pretraživanje po ključnim riječima, filtriranje i analizu datoteka. Ove funkcije olakšavaju identifikaciju relevantnih podataka i ubrzavaju proces pregleda velikih skladišnih sistema.

6. Identifikacija i analiza artefakata: The Sleuth Kit omogućava analizu različitih tipova artefakata, kao što su mrežni podaci, datoteke evidencija (log fajlovi), i razni tipovi metapodataka. Ovi podaci mogu ukazivati na aktivnosti kao što su instalacija programa, pristup fajlovima ili čak pokušaji prikrivanja aktivnosti.

7. Podrška za integraciju sa Autopsy-jem: TSK se često koristi u kombinaciji sa Autopsy-jem, koji predstavlja grafički interfejs za The Sleuth Kit. Autopsy nudi intuitivnu platformu koja olakšava analizu i vizualizaciju dokaza, kao i bržu preglednost nalaza.

8. Pristup informacijama o datotekama na nivou niskih slojeva: TSK omogućava istražiteljima pregled sadržaja datoteka na nižem binarnom nivou, što može otkriti podatke ili aktivnosti koje su sakrivene ili enkriptovane.

The Sleuth Kit se koristi prvenstveno u istragama na nivou državnih institucija, policije i privatnih forenzičkih firmi. Njegova popularnost dolazi iz fleksibilnosti, detaljne analize datotečnih sistema, i mogućnosti integracije sa drugim forenzičkim alatima.

Forenzika nasilnog ekstremizma u digitalnom okruženju

MVT

5

Norway

SMART Balkans
Civil Society for Shared Society in the Western Balkans

CPCD
Centar za promociju civilnog društva

IDM
Institute for Democracy and Mediation

CRPM
Center for Research and Policy Making
...policy impact since 2004

MVT (Mobile Verification Toolkit) je open-source alat razvijen prvenstveno za digitalnu forenziku mobilnih uređaja. Razvijen od strane Amnesty International i zajednice istraživača, MVT je dizajniran za detekciju potencijalnih sigurnosnih prijetnji na mobilnim uređajima, posebno onih povezanih sa naprednim špijunskim softverom kao što je Pegasus. Ovaj alat omogućava identifikaciju znakova kompromitovanja uređaja prisustva zlonamernih aktivnosti. Evo glavnih funkcionalnosti i primjena MVT-a:

1. Otkrivanje znakova kompromitovanja (IOC- Indicators of Compromise): MVT omogućava analizu podataka sa mobilnih uređaja kako bi otkrio indikatore kompromitovanja, kao što su sumnjive datoteke, procesi, i mrežne aktivnosti. Koristi IOC liste koje istraživači redovno ažuriraju kako bi pomogli u identifikaciji špijunskog softvera.

2. Analiza i dekodiranje sigurnosnih kopija uređaja: Alat može raditi sa sigurnosnim kopijama mobilnih uređaja, što omogućava forenzičarima da pregledaju podatke sa uređaja bez potrebe za direktnim fizičkim pristupom. MVT podržava analizu iOS i Android sigurnosnih kopija i omogućava dekodiranje različitih formata podataka.

3. Forenzička analiza aplikacija i logova: MVT analizira podatke iz različitih aplikacija i logove sistema kako bi identifikovao potencijalno sumnjive aktivnosti.

Na primjer, može analizirati podatke iz aplikacija za razmjenu poruka, email aplikacija i drugih softverskih komponenti koje mogu biti ciljane od strane napadača.

4. Identifikacija prisustva špijunskog softvera kao što je Pegasus: MVT je dizajniran specifično sa fokusom na identifikaciju špijunskog softvera koji kompromituje privatnost korisnika. Pruža mogućnost otkrivanja prisustva špijunskih softvera poput Pegasusa na osnovu poznatih šablona ponašanja i znakova kompromitovanja.

5. Izvoz i pregled rezultata analize: Nakon analize, MVT omogućava izvoz rezultata u preglednom formatu, poput CSV ili JSON formata. Ovi izvještaji se mogu koristiti za dalju istragu ili kao dokazi u pravnim procesima.

6. Usklađenost sa pravnim standardima: MVT generiše izveštaje i rezultate analize koji su korisni kao forenzički dokazi i u pravnim slučajevima, jer omogućavaju validaciju zaključaka putem transparentnog prikaza podataka.

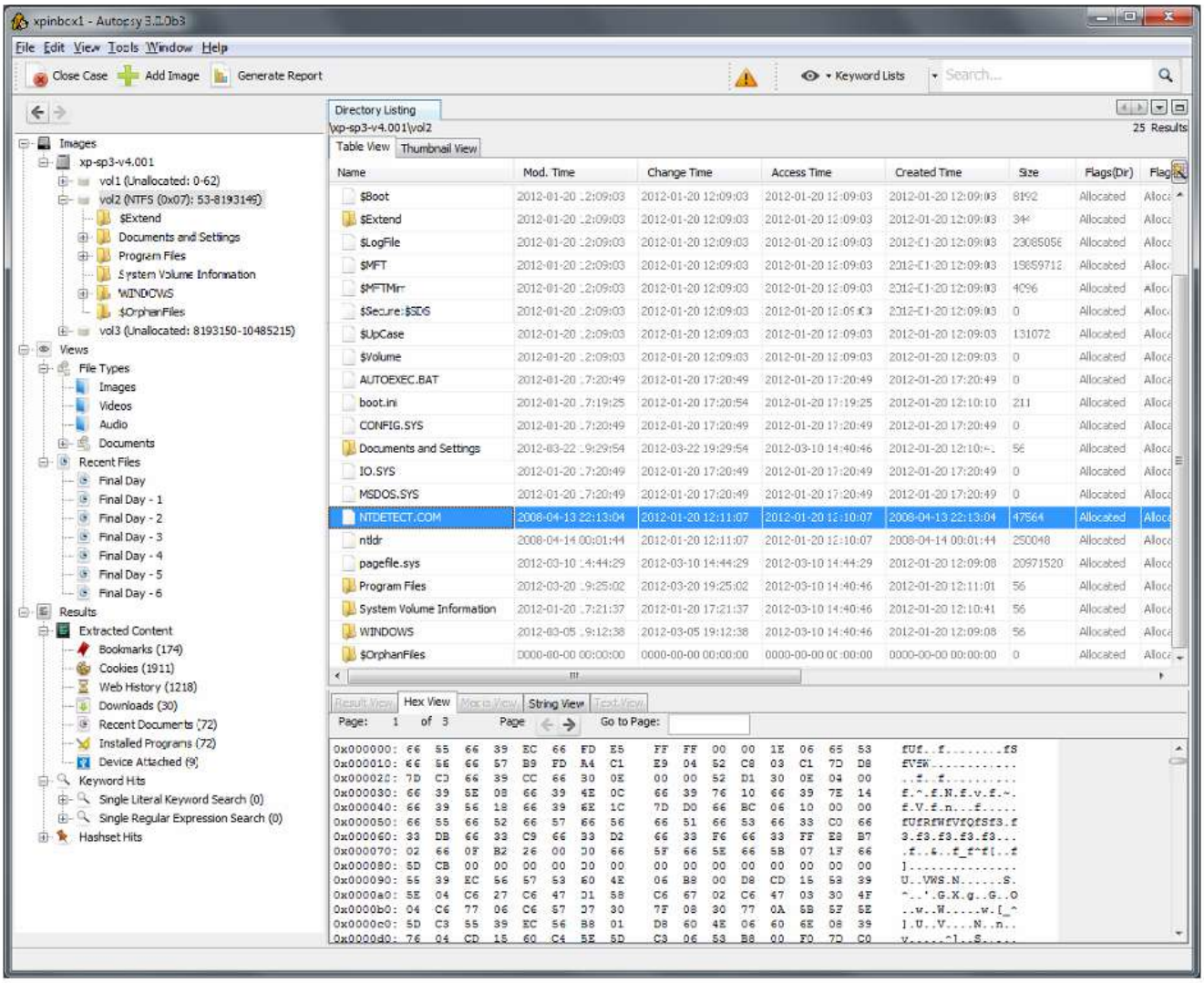
7. Podrška za rad u komandnoj liniji: MVT je alat koji funkcioniše u komandnoj liniji, što ga čini fleksibilnim i pogodnim za rad na različitim platformama (Linux, macOS, Windows). Može se koristiti za automatizovano skeniranje i analizu većeg broja uređaja ili sigurnosnih kopija.

MVT je posebno koristan alat za novinare, istraživače, i organizacije koje se bave ljudskim pravima, kao i za profesionalce u digitalnoj forenzici i cyber sigurnosti. Njegov primarni cilj je otkrivanje sofisticiranih pretnji koje ciljaju privatnost korisnika, a alat se konstantno unapređuje kako bi odgovarao rastućim pretnjama u svijetu mobilne sigurnosti.

Forenzika nasilnog ekstremizma u digitalnom okruženju

Autopsy

6



Autopsy je besplatan i open-source digitalni forenzički alat sa grafičkim interfejsom, razvijen za pregled i analizu digitalnih dokaza na skladišnim uređajima. Koristi se u istragama za prikupljanje i analizu podataka sa računara, tvrdih diskova, USB uređaja, i drugih medija. Autopsy je posebno popularan zbog svoje pristupačnosti i podrške za širok spektar forenzičkih analiza, a funkcioniše kao korisnički interfejs za alat The Sleuth Kit (TSK). Evo glavnih funkcionalnosti i primena alata Autopsy:

1. **Obnova obrisanih podataka**: Autopsy omogućava identifikaciju i rekonstrukciju obrisanih fajlova i direktorijuma, što je ključno u slučajevima kada je potrebno povratiti izbrisane dokaze ili analizirati tragove pokušaja skrivanja podataka.

2. **Analiza datotečnih sistema**: Podržava analizu različitih tipova datotečnih sistema, uključujući NTFS, FAT, Ext2/3/4, HFS+, i druge, što omogućava dubinsku forenzičku istragu. Pruža informacije o strukturi diska, particijama, i lokaciji podataka.

3. Pregled i analiza vremenskih oznaka: Autopsy može prikazati vremenske oznake povezane sa kreiranjem, modifikacijom i pristupom datotekama, što je korisno za rekonstrukciju događaja i identifikaciju aktivnosti na uređaju.

4. Internet forenzika: Alat ima ugrađene mogućnosti za analizu internet aktivnosti korisnika, uključujući pregled historije pretrage, keširanih fajlova, kolačića, i preuzetih fajlova sa popularnih web pregledača. Ovo može pružiti uvid u online aktivnosti korisnika.

5. Analiza elektronske pošte: Autopsy može analizirati datoteke povezane sa email klijentima, poput Microsoft Outlook i Mozilla Thunderbird. Omogućava pristup email porukama, prilozima, kontaktima i drugim podacima u vezi sa komunikacijom.

6. Identifikacija ključnih reči i pretraga po sadržaju: Korisnici mogu postaviti ključne riječi za pretragu u okviru svih podataka na disku, uključujući sadržaj datoteka i metapodatke. Ovo je korisno za brzo pronalaženje relevantnih informacija u velikim količinama podataka.

7. Analiza multimedijalnih datoteka: Autopsy omogućava pregled i analizu slika, videa i drugih multimedijalnih sadržaja, kao i detekciju potencijalno nedozvoljenih ili kompromitujućih sadržaja pomoću opcije prepoznavanja lica i drugih alata za vizuelnu analizu.

8. Modularna arhitektura sa dodatnim plugin-ovima: Autopsy ima podršku za različite dodatke koji proširuju njegove funkcionalnosti. Na primjer, dodatke za analizu memorije, detekciju zlonamernog softvera, i mrežnu forenziku, što ga čini veoma prilagodljivim alatima za različite vrste forenzičkih istraga.

9. Generisanje forenzičkih izveštaja: Alat omogućava automatsko kreiranje izveštaja u formatima kao što su HTML, PDF, i Excel, što olakšava pregled i prezentaciju dokaza. Izveštaji su strukturirani i prilagođeni za sudske postupke ili prezentaciju nalaza klijentima.

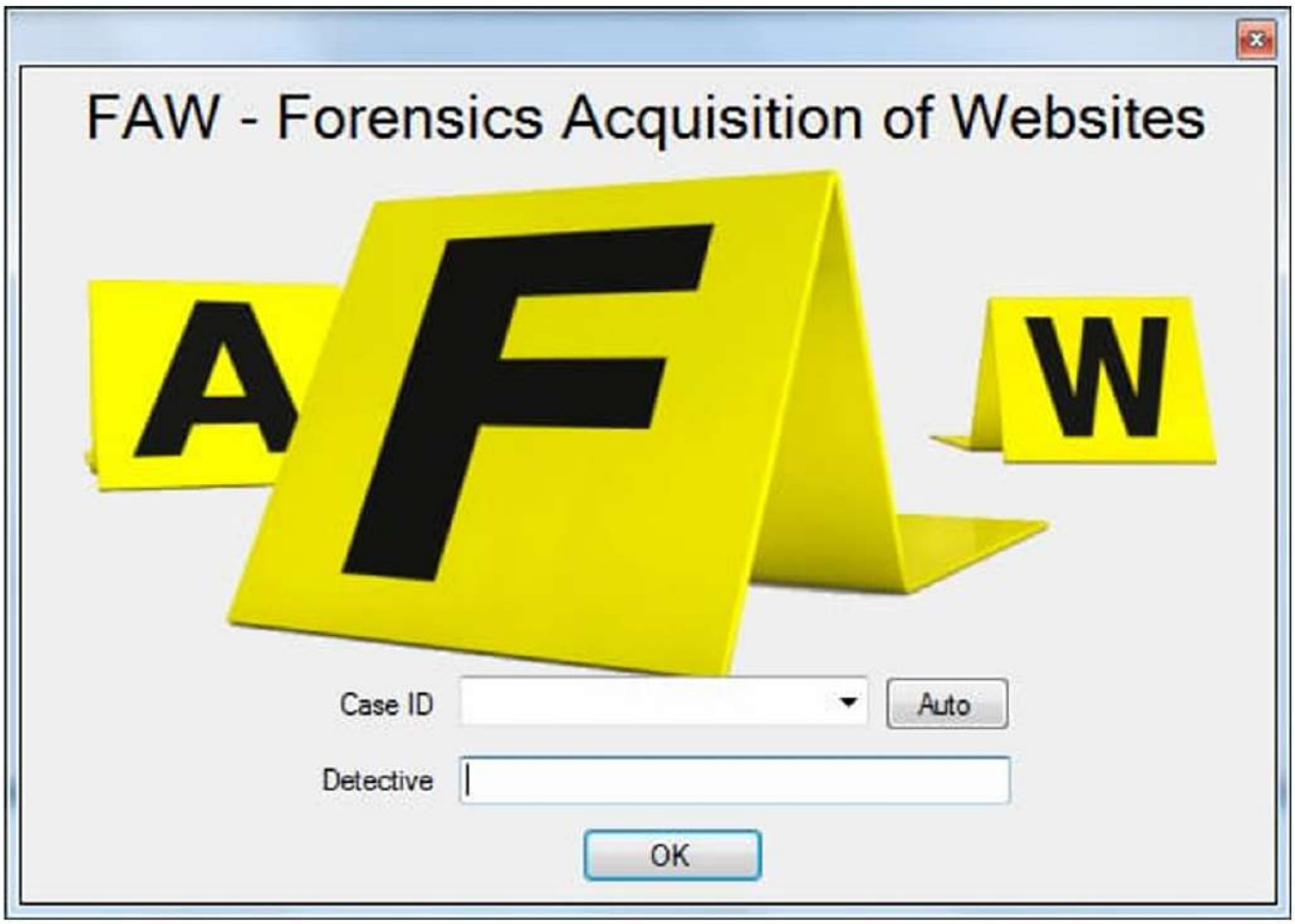
10. Intuitivan korisnički interfejs: Za razliku od mnogih forenzičkih alata, Autopsy nudi jednostavan i intuitivan grafički interfejs, što ga čini pogodnim za početnike, kao i za profesionalce. Alat omogućava pregled i analizu podataka kroz vizuelno prijatan i lako razumljiv prikaz.

Autopsy je široko korišćen u policijskim istragama, pravnim postupcima, i korporativnim istragama zbog svoje fleksibilnosti, širokog spektra funkcija, i pristupačnosti.

Forenzika nasilnog ekstremizma u digitalnom okruženju

FAW

7



FAW (Forensics Acquisition of Websites) je digitalni forenzički alat namenjen za akviziciju, odnosno prikupljanje i očuvanje sadržaja sa veb stranica na način koji osigurava integritet dokaza za kasniju analizu i upotrebu u pravnim procesima. Ovaj alat omogućava analizu online sadržaja, uključujući prikaz i prikupljanje dinamičkog sadržaja, što je važno za digitalne istrage u vezi sa internet prevarama, zlonamernim sajtovima, i drugim sajber prijetnjama. Evo ključnih primjena i funkcionalnosti FAW alata:

1. **Arhiviranje i snimanje web stranica**: FAW može sačuvati cjelokupnu strukturu veb stranice, uključujući HTML, CSS, JavaScript, slike, i ostale medijske datoteke. Ovaj sadržaj se čuva u forenzički prihvatljivom formatu, što osigurava očuvanje dokaza za dalju analizu ili sudski postupak.

2. **Prikupljanje dinamičkog sadržaja**: Alat omogućava snimanje dinamičkih elemenata web stranica koji se često mijenjaju, poput komentara, oglašavanja i sadržaja sa društvenih mreža. FAW omogućava akviziciju kompleksnih elemenata koji bi se inače izgubili prilikom jednostavnog snimanja ekrana.

3. Pridržavanje pravnih standarda: FAW prikuplja podatke na način koji je forenzički prihvatljiv, uključujući vremenske oznake i metapodatke, čime se osigurava dokazni integritet koji je potreban za pravne slučajeve.

4. Automatizacija prikupljanja sadržaja: Alat može automatski snimiti sadržaj sa određene web stranice na zadate vremenske intervale, što je korisno za kontinuirano praćenje promjena i dokumentovanje aktivnosti na sumnjivim sajtovima.

5. Kompatibilnost sa različitim formatima za eksport: FAW omogućava izvoz sačuvanog sadržaja u različite formate, kao što su PDF, CSV i HTML, što olakšava pregled i dijeljenje informacija sa timom ili klijentima.

6. Dokumentovanje URL-a i metapodataka: Osim samog sadržaja, FAW prikuplja i URL-ove, HTTP zaglavlja, kolačiće i druge metapodatke, čime se omogućava sveobuhvatna forenzička analiza veb aktivnosti.

7. Analiza u offline režimu: FAW omogućava analizu sačuvanih stranica offline, što je korisno za rad u okruženjima gde je pristup internetu ograničen ili kada je potrebno sačuvati podatke bez uplitanja u dalju interakciju sa sajtom.

8. Integracija sa drugim forenzičkim alatima: FAW se može integrisati sa drugim alatima za forenzičku analizu i istragu, kao što su alati za analizu mreže ili analizu sadržaja sa društvenih mreža, što omogućava sveobuhvatniji pristup digitalnim istragama.

FAW je posebno koristan u istragama gde je potrebno sačuvati web sadržaj kao dokaz, poput cyber kriminala, online prevara, i slučajeva kršenja prava intelektualne svojine.

Forenzika nasilnog ekstremizma u digitalnom okruženju

USB write blocker

USB Write Blocker je digitalni forenzički alat dizajniran da spreči zapisivanje podataka na USB uređaje tokom istrage ili analize. U digitalnoj forenzici, očuvanje integriteta dokaza je ključno, a USB Write Blocker osigurava da se podaci sa USB uređaja (poput eksternih tvrdih diskova, USB fleš memorija i drugih prenosnih medija) mogu pregledati i analizirati bez rizika od slučajnog ili namernog menjanja. Evo glavnih primjena i funkcionalnosti USB Write Blockera:

1. **Zaštita integriteta dokaza**: USB Write Blocker omogućava samo čitanje sa USB uređaja, blokirajući svaki pokušaj zapisivanja. Ovo sprečava slučajne promjene ili brisanje podataka sa USB uređaja, što je ključno u forenzičkim istragama za očuvanje originalnih podataka.

2. **Forenzička akvizicija podataka**: Omogućava bezbednu kopiju sadržaja sa USB uređaja za potrebe forenzičke analize, omogućavajući istražiteljima da naprave tačne kopije (imaging) bez modifikacije izvornog uređaja.

3. **Kompatibilnost sa različitim uređajima**: USB Write Blocker može raditi sa različitim vrstama USB uređaja, uključujući eksternu memoriju, SSD i HDD drajvove povezane putem USB-a. To ga čini univerzalnim rješenjem za različite vrste prenosnih uređaja.

4. Brza i jednostavna instalacija: Većina USB Write Blocker uređaja je dizajnirana kao "plug-and-play", što omogućava brzo postavljanje i upotrebu. To olakšava terensku forenzičku analizu i minimizuje potrebu za dodatnom opremom.

5. Kompatibilnost sa različitim operativnim sistemima: USB Write Blocker obično podržava rad sa različitim operativnim sistemima, uključujući Windows, macOS i Linux, čime je alat široko primjenljiv za istražitelje koji rade u različitim okruženjima.

6. Indikatori i obaveštenja: Većina Write Blocker uređaja dolazi sa LED indikatorima koji istražiteljima pokazuju status blokiranja zapisa. Ovo obezbjeđuje vizuelnu potvrdu da su sve operacije zapisivanja onemogućene i da je uređaj u sigurnom režimu za čitanje.

7. Podrška za rad sa forenzičkim softverom: USB Write Blocker se često koristi zajedno sa forenzičkim softverima kao što su EnCase, FTK, ili Autopsy, omogućavajući istražiteljima bezbjedan pristup USB uređajima unutar tih aplikacija bez rizika od mjenjanja podataka.

8. Zaštita od malicioznih aktivnosti: Blokiranjem pisanja, Write Blocker uređaj također pomaže u zaštiti istražiteljevog računara od potencijalno zaraženih fajlova sa analiziranog USB uređaja, što smanjuje rizik od širenja zlonamernog softvera.

USB Write Blocker je esencijalan alat u digitalnoj forenzici, jer osigurava integritet dokaza i omogućava bezbjedan pristup podacima za analizu. Koristi se u policijskim istragama, korporativnim istragama i laboratorijama za digitalnu forenziku, jer omogućava očuvanje podataka tokom čitavog procesa istraživanja.

Forenzika nasilnog ekstremizma u digitalnom okruženju

NFI Defraser

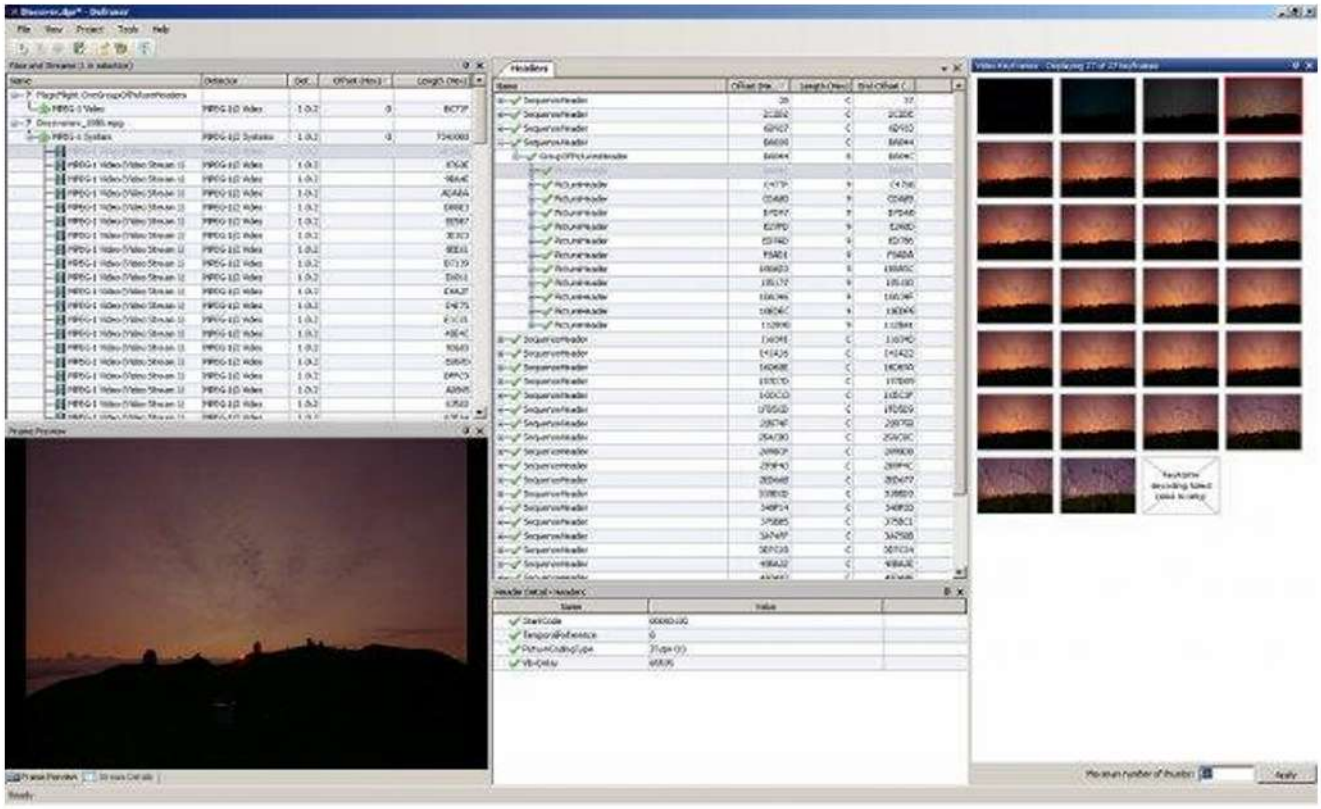
Norway

SMART Balkans
Civil Society for Shared Society in the Western Balkans

CPCD
Centar za promociju civilnog društva

IDM
Institute for Democracy and Mediation

CRPM
Center for Research and Policy Making
... making impact since 2004



NFI Defraser je forenzički alat razvijen od strane Nizozemskog forenzičkog instituta (NFI) za analizu i rekonstrukciju djelimično oštećenih ili fragmentiranih multimedijalnih datoteka, poput video i audio zapisa. Ovaj alat je posebno koristan u slučajevima kada su fajlovi oštećeni, djelimično izbrisani, ili su fragmentirani na disku, kao i u situacijama gde su dokazi namjerno manipulirani ili skrivani. Defraser omogućava istražiteljima da identifikuju i rekonstruišu multimedijalne fajlove iz različitih izvora, uključujući memorijske kartice, tvrde diskove i mrežne izvore. Evo glavnih funkcionalnosti i primjena alata NFI Defraser:

1. Analiza i rekonstrukcija video i audio fajlova: Defraser je specijalizovan za prepoznavanje, analizu i rekonstrukciju multimedijalnih datoteka (poput AVI, MP4, i drugih formata) koje su oštećene, fragmentirane, ili djelimično obrisane, čime se omogućava istražiteljima da dobiju ključne dokaze.

2. Prepoznavanje i rekonstrukcija fragmentiranih datoteka: Kada sumultimedijalne datoteke fragmentirane na disku, Defraser može analizirati fragmente i pokušati da ih spoji u cjelovitu datoteku. Ova funkcija je korisna kadase podaci nalaze u djelovima na različitim mjestima u memoriji ili na disku.

3. Podrška za razne multimedijalne formate: Alat može prepozn ati i analizirati različite formate, kao što su MPEG-1, MPEG-2, H.264, AVI, i MP4, omogućavajući fleksibilnost u istragama koje uključuju različite vrste multimedijalnih fajlova.

4. Analiza sadržaja podataka: Defraser analizira heksadecimalni sadržaj multimedijalnih datoteka kako bi identifikovao ključne strukture i metapodatke. Na taj način se mogu identifikovati manipulacije ili promjene u strukturi fajla koje mogu ukazivati na pokušaj skrivanja informacija.

5. Prikaz strukture fajla i identifikacija korupcije podataka: Alat prikazuje strukturu fajla na detaljan način, što omogućava istražiteljima da identifikuju dijelove datoteke koji su oštećeni ili nepravilno zapisani. To može biti korisno za razumevanje tačke korupcije i nivoa integriteta fajla.

6. Dokumentovanje rekonstrukcije i generisanje izveštaja: Defraser omogućava istražiteljima da kreiraju izveštaje o analizama koje uključuju podatke o vrsti fajla, pronadjenim fragmentima, i tačkama oštećenja. Izveštaji su struktuisani i pogodni za dalju analizu ili za pravne procese.

7. Integracija sa drugim forenzičkim alatima: Defraser može raditi zajedno sa drugim forenzičkim alatima, poput EnCase i FTK, čime se omogućava proširenje analitičkih kapaciteta i bolja preglednost dokaza.

8. Analiza sadržaja sa oštećenih uređaja: Defraser je koristan za slučajeve u kojima su podaci snimljeni na memorijske kartice, USB uređaje, ili druge medije koji su oštećeni ili namjerno manipulirani kako bi se sakrili dokazi.

NFI Defraser je važan alat u istragama gde su multimedijalni fajlovi oštećeni, izbrisani ili manipulirani, kao i u slučajevima gde je neophodno identifikovati dokaze koji su skriveni u fragmentima podataka.

fon edo

Forenzika nasilnog ekstremizma u digitalnom okruženju

Jabiheu

Paladin

10

Norway

SMART Balkans
Civil Society for Shared Society in the Western Balkans

CPCD
Centar za promociju civilnog društva

IDM
Institute for Democracy and Mediation
Institut për Demokraci dhe Ndërmjetësim

CRPM
Center for Research and Policy Making
...policy impact since 2004

Paladin je sveobuhvatan forenzički alat i platforma koja se koristi za prikupljanje, analizu i očuvanje digitalnih dokaza sa različitih uređaja. Paladin je razvijen od strane firme **PassMark Software** i predstavlja moćan alat u forenzičkim istragama, koji se koristi u radu sa računarima, mrežama i prenosivim uređajima. Glavna prednost Paladina je njegova sposobnost da pruži sveobuhvatan skup alata u jednom paketu, što istražiteljima omogućava da efikasno analiziraju i dokumentuju podatke, dok istovremeno održavaju integritet dokaza. Evo ključnih funkcionalnosti i primena Paladin alata:

1. **Kompletan set forenzičkih alata**: Paladin sadrži širok spektar ugrađenih alata za digitalnu forenziku, uključujući alate za disk imidžing (kopiranje diska bit po bit), analizu fajlova, pretragu metapodataka, analizu sistema fajlova, i još mnogo toga. Ovaj alat olakšava istražiteljima da rade sveobuhvatnu analizu bez potrebe za korišćenjem više različitih aplikacija.

2. **Forenzičko imidžing**: Paladin omogućava kreiranje bit po bit imidža diska, što znači da se tačno kopira sadržaj diska (uključujući obrisane datoteke, slobodan prostor i metapodatke). Ovaj imidž može biti kasnije korišćen za analizu bez ugrožavanja integriteta originalnog uređaja.

3. **Podrška za različite uređaje i sisteme**: Paladin podržava analizu različitih uređaja kao što su hard diskovi, SSD uređaji, USB uređaji, mobilni telefoni, i mrežni uređaji. Također, podržava različite operativne sisteme, uključujući Windows, macOS i Linux, što ga čini veoma fleksibilnim.

4. **Obnova obrisanih podataka**: Alat je specijalizovan za identifikaciju i povratak obrisanih datoteka i fajlova sa različitih uređaja, čime pomaže u obnavljanju ključnih dokaza koji mogu biti od presudnog značaja u istragama.

5. Forenzička analiza fajlova i metapodataka: Paladin omogućava dubinsku analizu fajlova, uključujući pregled metapodataka kao što su datum kreiranja, datum modifikacije, autora fajla, i druge važne informacije koje mogu pomoći u rekonstruisanju događaja.

6. Pretraga po ključnim riječima: Pruža mogućnost pretrage po ključnim riječima kroz veliku količinu podataka, što omogućava brzu identifikaciju relevantnih informacija u slučaju.

7. Analiza e-mailova i internet aktivnosti: Paladin također omogućava analizu podataka povezanih sa elektronskom poštom i internet aktivnostima, što je korisno u istraživanju prevara, internet kriminala ili drugih online aktivnosti.

8. Forenzičko računanje vremena: Pomoću Paladina moguće je precizno rekonstruisati događaje na računaru ili uređaju na osnovu vremenskih oznaka (timestamps) fajlova, sistemskih logova i drugih podataka koji mogu pružiti uvid u aktivnosti korisnika.

9. Dokumentovanje i izvještavanje: Paladin omogućava generisanje detaljnih izvještaja o svim analizama i otkrićima. Izvještaji su u formatu koji je pogodan za pravne postupke i forenzičku prezentaciju.

10. Linux Live CD/USB verzija: Jedna od karakteristika Paladina je njegova mogućnost pokretanja sa Live CD-a ili USB-a, što znači da istražitelji mogu koristiti alat za analizu bez potrebe za instaliranjem softvera na ciljani uređaj, čime se dalje čuva integritet dokaza.

11. Podrška za rad u timovima: Paladin omogućava saradnju više istražitelja kroz podešavanje zajedničkog radnog okruženja, čime omogućava lakše dijeljenje informacija i koordinaciju u velikim forenzičkim istragama.

Paladin je vrlo koristan u digitalnoj forenzici jer omogućava sveobuhvatan skup alata za analizu, dokumentaciju i očuvanje dokaza sa svih vrsta računarskih uređaja. On je idealan za forenzičare, policiju, istražitelje u vezi sa sajber kriminalom, kao i za organizacije koje se bave istražnim radom ili zaštitom podataka.

Forenzika nasilnog ekstremizma u digitalnom okruženju

VirusTotal

11

VirusTotal je popularna online platforma za analizu zlonamjernih fajlova, URL-ova i drugih digitalnih objekata. Alat koristi širok spektar antivirusnih motora i alata za skeniranje kako bi pružio detaljan izvještaj o potencijalnim pretnjama. Evo ključnih funkcionalnosti i primjena VirusTotal alata:

Ključne funkcionalnosti VirusTotal alata:

1. Skeniranje fajlova i URL-ova: VirusTotal omogućava korisnicima da učitaju fajlove ili unesu URL-ove kako bi ih analizirali pomoću više od 70 različitih antivirusnih motora i alata. To omogućava korisnicima da brzo detektuju malver ili zlonamjerne aktivnosti povezane sa tim fajlom ili URL-om.

2. Korišćenje više antivirusnih baza podataka: VirusTotal koristi mnoge različite antivirusne alate i motore, uključujući poznate brendove kao što su Kaspersky, McAfee, ESET, Sophos, i mnoge druge. Ovo omogućava da se fajl skenira iz više različitih perspektiva, što povećava tačnost detekcije.

3. Detekcija malvera i sumnjivih fajlova: Alat je efikasan u prepoznavanju širokog spektra malvera, uključujući viruse, trojance, ransomware, adware, špijunske programe (spyware), i druge oblike zlonamjernog softvera. Pruža rezultate skeniranja koji omogućavaju korisnicima da razumiju da li je fajl siguran ili predstavlja prijetnju.

4. Analiza metapodataka fajlova: VirusTotal pruža detaljne informacije o fajlovima, uključujući metapodatke kao što su veličina fajla, datum kreiranja, format fajla, i druge informacije koje mogu pomoći u analizi i procjeni bezbednosti.

5. Prepoznavanje sumnjivih URL-ova: Pored fajlova, VirusTotal omogućava skeniranje URL-ova kako bi se provjerilo da li su povezani sa malicioznim sajtovima. Ovo je korisno za detekciju phishing sajtova, sajber napada i drugih online pretnji.

6. Integracija sa drugim forenzičkim alatima: VirusTotal se često koristi u kombinaciji sa drugim forenzičkim alatima i platformama, omogućavajući analizu digitalnih dokaza i prepoznavanje sigurnosnih prijetnji unutar većih istraga.

7. Automatizacija skeniranja: VirusTotal nudi i API koji omogućava automatizovano skeniranje fajlova, što je korisno za organizacije koje žele da integrišu ovu funkcionalnost u svoje sisteme za detekciju malvera i bezbjednosne nadzore.

8. Pretraga po fajlovima: VirusTotal omogućava pretragu po prethodnim fajlovima koji su već analizirani, što omogućava istražiteljima da brzo provjeravaju fajlove koji su već prošli kroz skeniranje i da dobiju informacije o njihovom statusu.

9. Transparentnost i zajednička baza podataka: Jedna od prednosti VirusTotal-a je njegova transparentnost u vezi sa rezultatima skeniranja. Svi korisnici mogu da vide kako su različiti antivirusni motori detektovali fajl, što omogućava dublje razumjevanje prijetnje.

Primjene VirusTotal alata:

Forenzičke istrage: VirusTotal je vrlo koristan u digitalnim forenzičkim istragama, jer omogućava istražiteljima da brzo provjeravaju fajlove i URL-ove povezane sa potencijalnim malverom, phishing napadima, ili drugim oblicima sajber kriminala.

Testiranje sigurnosti: Organizacije i sigurnosni istraživači koriste VirusTotal za brzo testiranje fajlova i URL-ova u cilju identifikacije novih prijetnji ili analize već postojećih napada.

Proaktivna zaštita: VirusTotal može pomoći u prepoznavanju potencijalnih prijetnji pre nego što izazovu štetu, što je korisno za antivirusne firme, kompanije za sajber sigurnost, ili pojedince koji žele da zaštite svoje uređaje.

Saradnja u sajber bezbednosti: VirusTotal je takođe korisno oružje za saradnju među istražiteljima i bezbjednosnim stručnjacima, jer omogućava dijeljenje informacija o sumnjivim fajlovima i prijetnjama.

Prednosti VirusTotal-a:

Brza analiza i rezultati: VirusTotal pruža brze rezultate skeniranja, omogućavajući korisnicima da brzo odluče da li je fajl ili URL bezbjedan.

Besplatan pristup: Osnovne funkcionalnosti VirusTotal-a su besplatne, što ga čini dostupnim širokom broju korisnika, od pojedinaca do profesionalnih istražitelja.

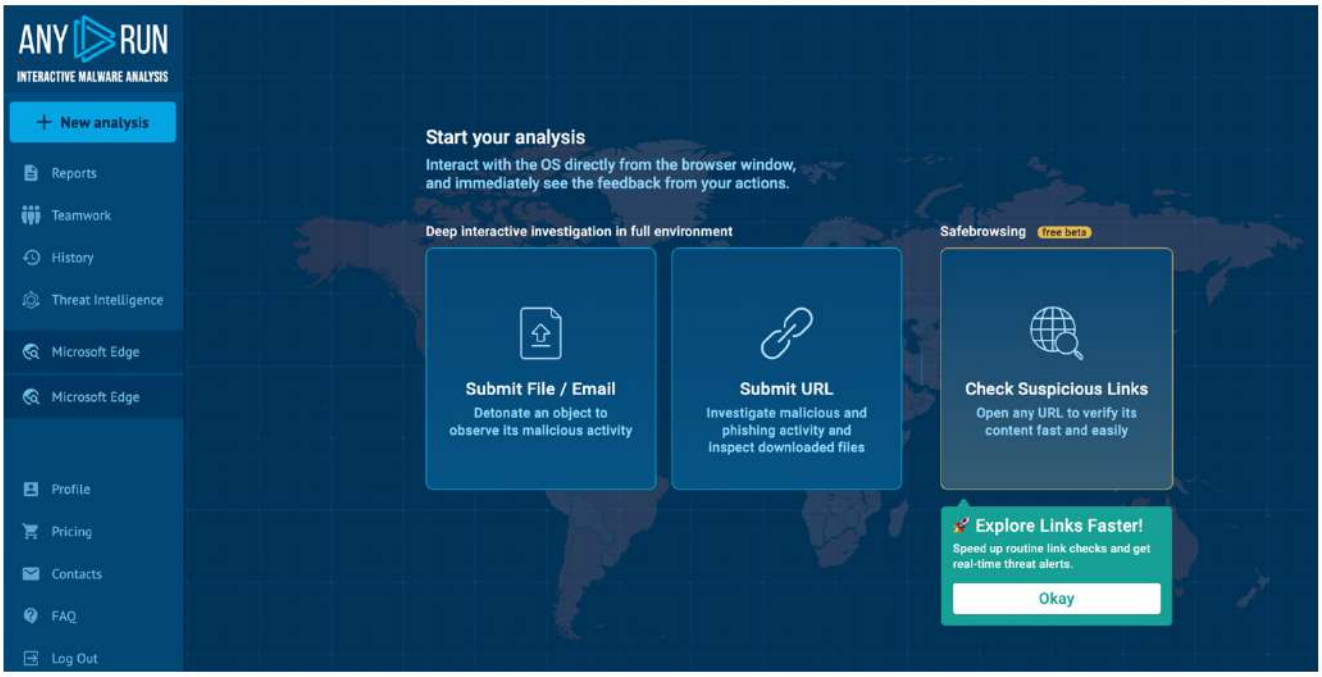
Podrška za razne formate: VirusTotal podržava analizu mnogih različitih fajl formata (npr. .exe, .pdf, .docx, .zip) i URL-ova.

VirusTotal je efikasan i popularan alat za detekciju zlonamjernih fajlova i URL-ova. Njegova sposobnost da koristi više antivirusnih motora za analizu i detaljan uvid u sigurnost fajlova čini ga korisnim alatom u digitalnoj forenzici, sajber sigurnosti, i svakodnevnoj zaštiti od malvera.

Forenzika nasilnog ekstremizma u digitalnom okruženju

AnyRun

12



AnyRun je alat za dinamičku analizu malvera koji omogućava praćenje njegovih aktivnosti u izolovanom okruženju (sandbox). Koristi se za detekciju i analizu ponašanja malvera, uključujući interakciju sa fajlovima, sistemom i mrežom.

Ključne funkcionalnosti:

1. **Dinamička analiza**: Pokreće malver u sigurnom okruženju i prati njegove aktivnosti u realnom vremenu.

2. **Mrežna analiza**: Detektuje mrežne veze malvera, uključujući komunikaciju sa komandnim serverima.

3. **Pratite promjene u sistemu**: Analizira promjene koje malver pravi na fajlovima, registrima i sistemskim podešavanjima.

4. **Interaktivnost**: Omogućava korisnicima da aktivno učestvuju u analizi i manipulišu okruženjem.

5. **Generisanje izveštaja**: Pruža detaljne izvještaje sa informacijama o ponašanju malvera.

Primjene:

Analiza malvera: Razumjevanje kako malver funkcioniše i komunicira.

Forenzičke istrage: Identifikacija prijetnji i dokaza za sajber napade.

Pronaći IOC (indikatore kompromitacije): Otkrivanje znakova malicioznih aktivnosti.

AnyRun je koristan alat za dubinsku analizu malvera, detekciju složenih prijetnji i istraživanje sajber napada.

Forenzika nasilnog ekstremizma u digitalnom okruženju

Projekat podržava SMART Balkan - Civilno društvo za povezan Zapadni Balkan, implementiraju Centar za promociju civilnog društva (CPCD), Center for Research and Policy Making (CRPM) i Institute for Democracy and Mediation (IDM) i finansijski podržava Ministarstvo vanjskih poslova Kraljevine Norveške.

Autori:

Ozrenko Đurić Branko Petrović Cyber wings team