



PERSEUS

PERSEUS TECHNOLOGY · DIGITAL FORENSIK



Perseus Explorer

Forensisk diskavbildning och djup filsystemsanalys

En komplett arbetsstation för disk- och minnesforensik: montera en avbildning eller en fysisk disk, rekonstruera filsystemet, återskapa det som raderats eller dolts, och ta fram en dokumenterad, domstolsfärdig rapport — allt på en Windows-dator, utan att data lämnar labbet.

8

filssystem, tolkade nativt

6+

avbildningsformat

110+

kurerade YARA-regler

3

flytande aktiveringar



```
examiner@perseus:~$ perseus --filesystems
```

```
NTFS · APFS · ext4 · FAT32 · exFAT · Btrfs · XFS · ReFS
```

```
examiner@perseus:~$ perseus --doctrine
```

```
larma högt · härkomst på varje värde
```

```
examiner@perseus:~$ perseus --yellowkey
```

```
skrivskyddad NTFS-fjärrbläddring · BitLocker med nyckel · verifierad överlämning
```

```
examiner@perseus:~$ perseus --evidence
```

```
ingenting lämnar labbet
```

Kärnfunktioner

Åtta filsystem, tolkade nativt

NTFS, APFS, ext4, FAT32, exFAT, Btrfs, XFS och ReFS — med MFT/inod-rekonstruktion, återställning av raderade filer och full härkomst på varje värde.

Alla vanliga avbildningsformat

Raw/dd, E01/EFW, VHD, VHDX, VMDK och QCOW2, samt direkt skrivskyddad åtkomst till fysiska diskar.

Lösenordsåterställning med flera motorer

BitLocker, LUKS, VeraCrypt, APFS FileVault samt PDF, Office och ZIP — med ordlisto-, regel- och maskattacker.

Detektionsmotorer

YARA (110+ kurerade regler), en Sigma-utvärderare över Windows-händelseloggar och en signaturlösningsdatabas som täcker 300+ filtyper.

Minnesforensik

Processrekonstruktion, rootkit-detektion via korsvy från flera kärnkällor, process-injektion och extraktion av TLS-nycklar.

Anti-forensik och dolda data-detektion

Tidsmanipulation, steganografi och en systematisk genomsökning efter dold data i alla åtta filsystem — slack, alternativa dataströmmar, reserverad metadata med mera.

USB- och flyttbar media-aktivitet

Rekonstruera vilka enheter som anslutits — först sedda, senast sedda, senast borttagna, och på Windows vilken användare — i Windows, Linux och macOS, med härkomst på varje värde och källartefakten namngiven.

Carving och återställning

En flerstegs signatur- och entropi-carver, råsektorsökning och MFT-baserad återställning av raderade filer.

Fjärrinsamling, på ditt eget nätverk

Boota ett målsystem via din egen switch (PXE) och avbilda tillbaka till arbetsstationen, eller hämta från en fjärrvärd över SSH — varje steg spärrat av en registrerad behörighet.

Skrivskyddad fjärråtkomst till bevis

Bläddra i ett måls NTFS-partition över den certifikat-pinnade agentlänken och exportera valda filer med egen rapport och omläst hash — utan att röra källan. Läs BitLocker-klartext med ett giltigt återställningslösenord, utan montering eller skrivbar mappning.

Verifierad bevisöverlämning

Försegla bevis, deras ursprungsrapporter och en kundläsbar sammanfattning i ett hashat paket; varje del omverifieras oberoende och leveransen kontrolleras mot en oberoende kontrollsumma.

Rapportering och ärendehantering

HTML- och PDF-rapporter, en icke-redigerbar verifieringskedja, en bevisgraf och en ärendehanterare.

AI-assisterad utredning, redo för luftgap

Valfri analysassistent med strikt datapolitik — inklusive ett lokalt läge där ingenting lämnar datorn.

Där Perseus Explorer visar sitt värde

Varje utredare minns fallet som avgjordes av en enda fil som någon var säker på hade försvunnit.

Filen som var "borta"

En forskare tömmer fel mapp två dagar före inlämning — och senaste backupen togs för en vecka sedan. Du ansluter disken skrivskyddad, och inom några minuter återskapar Perseus Explorer filen direkt ur filsystemets egna register: intakt, tidsstämplad och bärd av en hash du kan bevisa. Paniken i rummet blir till lättnad — och du har gjort det utan att röra originalet.

Disken som såg ren ut

Det gör den oftast. Men i samma ögonblick som du kör dolldata-genomsökningen lyfter Perseus fram vad slack, alternativa dataströmmar och reserverad metadata tyst höll — i alla åtta filsystem, på de ställen de flesta verktyg aldrig tänker leta. Det som var osynligt för en minut sedan ligger nu på bordet, dokumenterat och försvarbart.

Klockan 02, och nätverket brinner

Ditt incidentteam kallas till ett pågående intrång. Medan avbildningen strömmar tillbaka över din egen switch — inget moln, ingen väntan — carvar du redan minnet efter den injicerade processen och drar USB-historiken som visar exakt vilken enhet som bar ut datan, och när. När kunden frågar "vad hände?" har du redan svaret.

Föreställ dig nästa disk som landar på ditt skrivbord. Du öppnar den en gång i Perseus Explorer, tidslinjen bygger sig själv, och svaret du behövde finns där — framför dig, redo att rapporteras. Så förtjänar verktyget sin plats.

Det som utmärker

- [✓] Systematisk dolldata-detektion i alla åtta filsystem — inte en eftertanke för ett enda filsystem.
- [✓] Forensisk ärlighet i grunden: varje värde bär sin härkomst (Verifierad, Härledd, Degraderad eller Otillgänglig), och verktyget larmar hellre än fabricerar ett resultat.
- [✓] En insamlingsplattform i fält på en laptop plus en nätverksswitch — ingen separat server, inget moln, ingen tredje part i beviskedjan.
- [✓] En flytande licens som följer utredaren, inte datorn, med ett helt offline-läge för luftgapade labb.

BYGGD FÖR Oberoende DFIR- och incidentkonsulter · Interna SOC- / CIRT- / CSIRT-team · Polisens digitala enheter · Företagsutredningar, HR & internrevision · Forensiska labb & sakkunniga · IT- och dataräddningsspecialister · Forskare, journalister & fotografer som helt enkelt behöver filen tillbaka

I korthet

Plattform	Windows 10 / 11 (64-bit)
Filsystem	NTFS · APFS · ext4 · FAT32 · exFAT · Btrfs · XFS · ReFS
Avbildningar	raw/dd · E01 · VHD · VHDX · VMDK · QCOW2 · fysiska diskar
Distribution	Fristående skrivbord; flytande licens, offline-alternativ
Datahantering	Helt lokal; valfri AI med luftgapat läge

Ärligt om omfånget

Perseus Explorer riktar sig till den arbetande utredaren och DFIR-konsulten, med fokus på forensiskt djup på bevis du själv förfogar över. RAID 0/1/5 rekonstrueras; vissa funktioner är medvetet avgränsade och redovisas som sådana i stället för att approximeras — verktyget presenterar aldrig ett härlett resultat som verifierat.

Licensiering

En licens per produkt, tre simultana aktiveringar som flyttar mellan datorer (en utredare för Detect). Standardnivån låser upp alla funktioner. En 30-dagars online-heartbeat håller aktiveringarna ärliga; en helt offline-licens finns för luftgapade labb. Ingenting om dina bevis når någonsin Perseus.

Fler verktyg i Perseus-serien

Perseus iPhone Backup Analyzer

Forensisk analys av iOS-backuper och enheter

Perseus Detect

Detektion av övervakning och avancerad spionprogramvara på iOS

Öppna en enda avbildning, så förstår du varför utredare håller Perseus Explorer inom räckhåll. Det här är ett verktyg du vill ha i din verktygslåda.

perseustechnology.se