

تکنیک‌های مستندسازی امن اعتراضات و رویدادها

صدای امن
sv.khro.org





فهرست

- **مقدمه**
- **فصل اول:** اخلاق و امنیت دوربین در میدان
- **فصل دوم:** روش‌های پنهان‌سازی و ویرایش امن تصاویر
- **فصل سوم:** پاک‌سازی ریشه‌ای ردپای دیجیتال
- **فصل چهارم:** راه‌های ذخیره امن و جاسازی محرمانه اطلاعات
- **فصل پنجم:** روش‌های ارتباط امن و قفل‌گذاری حساب‌ها
- **سخن پایانی**



مقدمه

در دکترین امنیت مدرن، تفکیک میان «امنیت در کف خیابان» و «امنیت در بستر شبکه»، یک خطای استراتژیک، مهلک و غیرقابل‌جبران است. ارگان‌های سرکوبگر از جمله پلیس فتا، واجا و اطلاعات سپاه، فرآیند شناسایی و سرکوب را از حالت سنتی به یک چرخه هوشمند، متصل و داده‌محور *(Data-Driven)* تبدیل کرده‌اند. این چرخه شامل چهار ضلع اساسی است: ثبت تصویر در میدان، استخراج هویت فیزیکی از طریق هوش مصنوعی، تتبع ردپای دیجیتال در شبکه‌های اجتماعی، و در نهایت بازداشت فرسایشی فعالان.

در اقلیم اهواز *(استان خوزستان)*، به دلیل تکرار قطعی‌های سراسری اینترنت در زمان بحران‌های محیط‌زیستی *(مانند بحران آب و انتقال کارون)* و اعتراضات معیشتی-مدنی، مستندسازی نقض حقوق بشر با چالش «پنهان‌کاری سیستماتیک» مواجه است. هدف این راهنما، تسلیح تکنولوژیک شماست؛ به‌گونه‌ای که لنز دوربین خود را به یک سپر دفاعی تبدیل کنید تا حقیقت ثبت و مخابره شود، اما راوی و سوژه هرگز در رادار نظارتی دستگاه سرکوب قرار نگیرند.



فصل اول

اخلاق و امنیت دوربین در میدان

تصویربرداری میدانی در مناطق بحرانی، صرفاً فشردن دکمه ضبط نیست؛ یک فرآیند مهندسی‌شده است که باید کمترین متادیتای بصری و هویتی را به ناظر سرکوبگر ارائه دهد.

1.1. آناتومی خطرات بینایی ماشین (Computer Vision)

سیستم‌های نظارتی مدرن و دوربین‌های ثبت تخلفات شهری ترافیکی که در تقاطع‌های اصلی و محلات اقلیم اهواز نصب شده‌اند، دیگر متکی به نگاه اپراتور انسانی نیستند. این سیستم‌ها مجهز به الگوریتم‌های پیشرفته تشخیص چهره (Face Recognition)، تشخیص پلاک (ANPR) و تحلیل ویژگی‌های فردی (Soft Biometrics) مانند قد، فرم شانه و نحوه گام‌برداری (Gait Analysis) هستند.

پروتکل پوشش بیومتریک در میدان

استفاده از ماسک‌های پزشکی به تنهایی بی‌فایده است؛ زیرا هوش مصنوعیِ نظارتی می‌تواند با تقارن‌سازی استخوان پیشانی، فاصله چشم‌ها و بازسازی بقیه صورت، هویت را حدس بزند. فعالان باید از تکنیک لایه‌بندی بصری استفاده کنند:

الف) **عینک‌های آفتابی کاملاً مات و بدون رفلکس**

برای پنهان کردن کاسه چشم و نقطه تمرکز الگوهای بیومتریک.

ب) **کلاه‌های لبه‌دار بلند (بیسبال/آفتابی)**: برای شکستن زاویه دید دوربین‌های نصب‌شده در ارتفاع بالا و ایجاد سایه روی نیمه فوقانی صورت.

پ) **ماسک‌های پارچه‌ای تیره رنگ و بدون طرح**: ماسک باید تا زیر چانه را بپوشاند تا فرم فک (Jawline) که یکی از شاخص‌های اصلی بینایی ماشین است، کاملاً مخدوش شود.





1.2. سناریوی تحلیل بازتاب نور

یکی از پیچیده‌ترین و مهجورترین روش‌های شناسایی فرستندگان ویدیو توسط بخش فنی پلیس فتا، آنالیز بازتاب‌های ناخواسته در تصاویر (Reflection Forensics) است.

هنگام فیلم‌برداری مخفیانه از پشت پنجره یک ساختمان، داخل مغازه یا از درون خودرو، شیشه مانند یک آینه نیمه‌شفاف عمل می‌کند. تصویر چهره شما، مدل یا رنگ لباس شما، یا دکوراسیون داخلی اتاق بر روی شیشه منعکس و هم‌زمان با صحنه بیرونی ضبط می‌شود. ابزارهای پردازش تصویر با تقویت کنتراست (Contrast Enhancement) این بخش‌ها، مأموران را مستقیماً به اتاق یا خودروی فرستنده می‌رسانند.

قبل از شروع فیلم‌برداری از پشت شیشه، تمام منابع نوری پشت سر خود (چراغ اتاق، نمایشگر لپ‌تاپ، ال‌سی‌دی تلویزیون یا گوشی دوم) را کاملاً خاموش کنید. اتاق باید در تاریکی مطلق باشد.

لنز دوربین گوشی را به صورت کاملاً چسبیده و عمود بر سطح شیشه قرار دهید. استفاده از یک پارچه تیره دور لنز برای کور کردن روزنه‌های ورود نور جانبی، الزامی است.

از فیلم‌برداری از بدنه براق خودروهای پارک‌شده یا آینه‌های جانبی که ممکن است رد و تصویر شما را ثبت کنند، پرهیز کنید.

1.3. کارگاه تخصصی استتار صوتی

صداها به اندازه اثر انگشت، هویتی و منحصربه‌فرد هستند. الگوریتم‌های شنود فرکانسی می‌توانند زیست‌سنجی صدای افراد (Voiceprint) را با بانک اطلاعاتی صداهای ضبط‌کننده مخابراتی (اپراتورهای همراه اول و ایرانسل) تطبیق دهند.

نشانگرهای جغرافیایی صوتی (Acoustic Landmarks): صدای بوق یک قطار، صدای اذان از یک مسجد خاص با فرکانس مشخص، صدای ترانس برق محلی، لهجه منحصربه‌فرد فرستنده یا صدا زدن یک نام کوچک در پس‌زمینه فیلم، محدوده جغرافیایی و هویت شبکه را فاش می‌کند.

پروتکل عملیاتی: در زمان ضبط فیلم در میدان، تحت هیچ شرایطی صحبت نکنید و با اشاره دست با همراهان ارتباط برقرار کنید. قبل از ارسال یا انتشار فایل، با استفاده از نرم‌افزارهای ویرایشگر (مانند ساندویو یا ابزارهای داخلی پیام‌رسان‌ها)، صدای اصلی محیط را کاملاً قطع (Mute) کنید. هیچ فرکانس صوتی اصیلی نباید به خروجی نهایی راه یابد.



فصل دوم

روش‌های پنهان‌سازی و ویرایش امن تصاویر

هنگام انتشار تصاویر، محو کردن چهره معترضان یا مأموران سرکوب (جهت جلوگیری از شناسایی معترضان جانبی) یک الزام است. اما روش‌های سنتی کارایی ندارند.



فصل سوم

پاک‌سازی ریشه‌ای ردپای دیجیتال

فایل‌های شما تنها تصویر یا صدا نیستند، آن‌ها حامل یک «شناسنامه دیجیتال» پنهان‌اند. هر عکس یا ویدیویی که ضبط می کنید، به‌طور خود کار حاوی مختصات دقیق جغرافیایی، زمان ثبت و مدل دستگاه شماست. در د کترین نظارت هوشمند، پلیس برای ردیابی شما نیازی به تحلیل محتوای فیلم ندارد، آن‌ها فقط با خواندن این «ردپای پنهان»، هویت و موقعیت شما را استخراج می کنند. قبل از انتشار هر فایل، باید این پیوندهای دیجیتالی را به صورت ریشه‌ای نابود کنید تا دوربین شما، هیچ ردی از شما بر جای نگذارد.





3.1. تگ‌های پنهان خطرساز در فایل‌ها (EXIF Data)

هر تصویری که با گوشی هوشمند ثبت می‌شود، به طور خودکار حاوی یک شناسنامه دیجیتال به نام **EXIF** است. این شناسنامه شامل اطلاعات فوق‌امنیتی زیر است:

- **مختصات دقیق جغرافیایی ثبت عکس (Geotagging بر پایه GPS با دقت سانتی‌متر).**
- **زمان و تاریخ دقیق ثبت فریم (Timestamp).**
- **مدل دقیق دستگاه، شماره سریال سنسور دوربین و نسخه سیستم‌عامل.**

اگر این فایل با همین ساختار به دست پلیس فتا برسد، آن‌ها نیازی به تحلیل محتوای عکس ندارند؛ بلکه متادیتا مستقیماً هویت مالک و موقعیت دقیق او را افشار می‌سازد.

3.2. کارگاه عملی کلیک‌به‌کلیک Scrambled Exif (اندروید)

این ابزار یک اپلیکیشن متن‌باز، بدون تبلیغات و کاملاً آفلاین برای تخلیه متادیتا پیش از اشتراک‌گذاری فایل‌هاست:

الف) اپلیکیشن **Scrambled Exif** را از مخازن امن (مانند F-Droid) دانلود و نصب کنید.

ب) برنامه را باز کرده و در بخش تنظیمات (Settings)، گزینه‌های زیر را فعال کنید:

- Pick random filename (تغییر نام فایل به یک رشته کد تصادفی جهت حذف ردپای نام‌گذاری گوشی).
- Remove GPS Data و Remove Camera Data.

پ) حال به گالری گوشی خود بروید، عکس حساس را انتخاب کنید و دکمه **Share (اشتراک‌گذاری)** را بزنید.

ت) از میان برنامه‌ها، **Scrambled Exif** را انتخاب کنید. برنامه در کسری از ثانیه متادیتا را نابود کرده و منوی اشتراک‌گذاری دوم را باز می‌کند.

ج) اکنون فایلِ پاک‌سازی‌شده را از طریق پیام‌رسان امن ارسال کنید.



3.3. کارگاه متادیتا برای دسکتاپ با ابزار ExifTool (ویندوز و لینوکس)

الف)سیستم‌عامل ویندوز (بدون نصب هیچ برنامه‌ای):
یک راه خیلی ساده‌تر و بدون دانلود برنامه در ویندوز این است که روی عکس راست‌کلیک کنید، گزینه Properties را بزنید، به تب Details بروید و در پایین پنجره روی عبارت Remove Properties and Personal Information کلیک کنید؛ سپس گزینه دوم یعنی Remove the following properties from this file را انتخاب کرده، تیک همه را بزنید و تایید کنید.

ب)برای روزنامه‌نگارانی که حجم بالایی از فایل‌ها را روی کامپیوتر پردازش می‌کنند، ابزار تحت ترمینال **ExifTool** قدرتمندترین گزینه است:

- ترمینال (در لینوکس) یا Command Prompt (در ویندوز) را باز کنید.
- برای پاک‌سازی کامل و بدون بازگشتِ تمامی متادیتای موجود در یک پوشه حاوی اسناد و ویدیوها، دستور زیر را تایپ کرده و اجرا کنید:

```bash
exiftool -all= -overwrite_original /path/to/your/folder
```

توضیح سوئیچ‌ها: -all= به معنای حذف تمامی تگ‌ها و -overwrite_original به معنای بازنویسی روی فایل اصلی بدون ذخیره نسخه پشتیبانِ حاوی متادیتا است.



فصل چهارم

راه‌های ذخیره امن و جاسازی محرمانه اطلاعات

اگر دستگاه شما (گوشی یا لپ‌تاپ) در گشت‌های تفتیش خیابانی، ایست‌بازرسی‌ها یا هجوم به منزل مصادره شود، حذف ساده فایل‌ها (Delete) یا حتی بازگشت به تنظیمات کارخانه (Factory Reset) بی‌فایده است. نهادهای امنیتی با استفاده از سخت‌افزارها و نرم‌افزارهای ریکاوریِ فارنزیک (مانند دستگاه‌های Cellebrite که مستقیماً حافظه فیزیکی را کپی می‌کنند)، قادرند فایل‌های ماه‌ها پیش را نیز بازیابی کنند. در این شرایط، تنها راه نجات، استفاده از رمزنگاری غیرقابل‌شکست، پنهان‌نگاری و سیستم‌های امحای خودکار است.

4.1. کارگاه جامع VeraCrypt و دکترین «انکار باورپذیر»

نرم‌افزار **VeraCrypt** استاندارد طلایی رمزنگاری دسکتاپ است که از دکترین انکار باورپذیر پشتیبانی می‌کند. این تکنیک به شما اجازه می‌دهد یک گاوصندوق دیجیتال دو لایه بسازید.

- **ساختار گاوصندوق دو لایه:**

لایه خارجی (Outer Volume) با یک رمز عبور معمولی باز می‌شود. شما در این لایه فایل‌های عادی و بی‌خطر (مانند جزوات دانشگاهی یا فیلم‌های سینمایی) را قرار می‌دهید.

لایه مخفی (Hidden Volume) در دلِ لایه خارجی جاسازی شده است. این لایه هیچ نشانه‌ای از وجود خود نشان نمی‌دهد و با یک رمز عبور فوق‌العاده قوی باز می‌شود. تمام اسناد، ویدیوهای خام اعتراضات و لایسنس‌های پروژه در اینجا ذخیره می‌شوند.

- **پروتکل تقابل در بازجویی:** اگر تحت فشار شدید امنیتی مجبور به فاش کردن رمز عبور شدید، فقط رمز عبور لایه خارجی را به بازجو می‌دهید. سیستم لایه خارجی را باز می‌کند و مأموران فایل‌های بی‌خطر را می‌بینند. از نظر ریاضی و الگوریتم‌های رمزنگاری، هیچ روشی وجود ندارد که بازجو بتواند اثبات کند لایه دومی (لایه مخفی) نیز در آن فضا وجود دارد. وجود آن کاملاً انکارپذیر است.

4.2.راهکارهای رمزنگاری پیشرفته در پلتفرم موبایل

از آنجا که VeraCrypt مختص کامپیوتر است، برای پیاده‌سازی معماری امن در گوشی‌های هوشمند، ابزارهای زیر توصیه می‌شوند:

- **اپلیکیشن EDS NG (سیستم‌عامل اندروید):** این برنامه کامل‌ترین و قدرتمندترین ابزار برای شبیه‌سازی استانداردهای وراکریپت در موبایل است. EDS NG به شما اجازه می‌دهد کانتینرهای رمزنگاری‌شده‌ای (Volumes) که در کامپیوتر ساخته‌اید را مستقیماً در گوشی باز کرده، مدیریت کنید و همان سطح از امنیت و قابلیت «انکار باورپذیر» را در میدان همراه داشته باشید.
- **نرم‌افزار Cryptomator (رمزنگاری فایل‌محور):** برخلاف وراکریپت که یک «گاوصندوق یکپارچه» می‌سازد، Cryptomator فایل‌ها را به‌صورت تک‌به‌تک رمزنگاری می‌کند. این ابزار برای کنشگرانی که مجبور به استفاده از فضاهای ابری متداول (مانند Google Drive) هستند، حیاتی است. پیش از آپلود، فایل‌ها در گوشی رمزگذاری می‌شوند تا هیچ نهاد واسطی به محتوای آن‌ها دسترسی نداشته باشد.

4.3. کلیدهای مرگ و امحای اضطراری (Panic Buttons)

در بسیاری از مواقع، بازداشت در کف خیابان به صورت ناگهانی رخ می‌دهد و شما فرصت پاک کردن فایل‌ها را ندارید. در اینجا باید سیستم را برای «خودتخریبی» آماده کرده باشید.

اپلیکیشن Ripple (ریپل): یک اپلیکیشن متن‌باز است که به عنوان «دکمه وحشت» عمل می‌کند. می‌توانید تنظیم کنید که در صورت فشردن یک دکمه خاص روی صفحه، یا با سه بار فشردن سریع دکمه پاور گوشی، نرم‌افزار به صورت خودکار پیام‌رسان‌های حساس را پاک کند، از حساب‌های کاربری خارج شود و فایل‌های مشخصی را نابود کند.

پروتکل رمز عبور فریب (Duress PIN): برخی سیستم‌عامل‌های امنیتی به شما اجازه می‌دهند یک رمز عبورِ دروغین تنظیم کنید. اگر هنگام بازداشت مأموران از شما خواستند قفل گوشی را باز کنید و این رمز فریب را وارد کنید، گوشی به جای باز شدن، فوراً به تنظیمات کارخانه برمی‌گردد و تمام اطلاعات به صورت بازگشت‌ناپذیر پاک می‌شود (Wipe).

4.4. انتقال سریع به بایگانی ابریِ دانش‌صفر (Zero-Knowledge Cloud)

یک قانون طلایی در مستندسازی بحران وجود دارد و آن این است که دستگاه فیزیکی شما (گوشی یا دوربین) نباید محل نگهداری طولانی‌مدت اطلاعات باشد.

به محض ثبت تخلفات حقوق بشری و بازگشت به نقطه امن، باید فایل‌ها را به یک فضای ابری که از معماری «دانش‌صفر» بهره می‌برد منتقل کنید و سپس آن‌ها را از روی دستگاه فیزیکی خود کاملاً نابود سازید. استفاده از Proton Drive یا ارسال مستقیم از طریق بستر OnionShare در شبکه تور پیشنهاد می‌شود. در این سرویس‌ها، فایل‌ها قبل از خروج از دستگاه شما با پروتکل (E2EE) رمزنگاری می‌شوند. حتی اگر سرورهای این شرکت‌ها هک شوند، آن‌ها چیزی جز مجموعه‌ای از کدهای رمزنگاری‌شده در اختیار ندارند، زیرا کلید باز کردن این گاوصندوق تنها در ذهن شماست.





5.1. معماری لایه‌ای شبکه پیازی (Tor) و سکیوردراپ

برای ارسال اسناد نقض حقوق بشر به سازمان‌های بین‌المللی، هرگز نباید از مرورگرهای عادی (Chrome یا Safari) استفاده کنید، زیرا آدرس IP شما در سرورهای واسط ثبت می‌شود.

- **شبکه پیازی (Tor):** ترافیک شما را از سه لایه سرور تصادفی و رمزنگاری‌شده در سراسر جهان (Relays) عبور می‌دهد. سرور اول آدرس IP شما را می‌داند اما محتوا را نمی‌بیند؛ سرور دوم هیچ‌کدام را نمی‌داند؛ و سرور سوم (Exit Node) محتوا را به مقصد می‌رساند اما منبع اصلی را نمی‌شناسد.
- **سکیوردراپ (SecureDrop):** پلتفرمی پیازپایه (.onion) است که آژانس‌های حقوق بشری برای دریافت اسناد از افشاگران استفاده می‌کنند. با ورود به مرورگر تور و وارد کردن آدرس اختصاصی سکیوردراپِ سازمان هدف، می‌توانید اسناد را بدون بر جای گذاشتن کوچکترین ردپای دیجیتالی بارگذاری کنید.

5.2. کارگاه فعال‌سازی شبکه مش آفلاین با بریر (Briar)

در سناریوی تاریکی مطلق اینترنت (Internet Blackout) در خوزستان، پیام‌رسان **Briar** شریان ارتباطی هسته‌های میدانی را حفظ می‌کند. این برنامه نیازی به سرور مرکزی و اینترنت ندارد و از طریق وای‌فای محلی (بدون اینترنت) و بلوتوث، پیام‌ها را به صورت زنجیره‌ای (Mesh Network) بین گوشی‌ها جابه‌جا می‌کند.

نکته: سیستم‌عامل اندروید برای کاهش مصرف باتری، برنامه‌های پس‌زمینه را به صورت تهاجمی می‌بندد که این امر باعث قطع شبکه مش بریر می‌شود. برای واکسیناسیون برنامه:

a. به تنظیمات گوشی بروید: Settings > Apps > Briar.

b. وارد بخش **Battery** (یا App Battery Usage) شوید.

حالت مصرف را از Optimized به **Unrestricted** (بدون محدودیت) تغییر دهید. با این کار، بریر به صورت ۲۴ ساعته در پس‌زمینه روشن می‌ماند و دکل ارتباطی شما با دیگر اعضای شبکه قطع نخواهد شد.

5.3. پروتکل کامل واکسیناسیون حساب‌های کاربری

برای جلوگیری از کنترل حساب‌های تلگرام، واتس‌اپ و شبکه‌های اجتماعی پس از مصادره سیم‌کارت یا هک شبکه‌ای، اعمال این سه خط دفاعی اجباری است:

- **حذف احراز هویت پیامکی (SMS 2FA):**
اپراتورهای داخلی به دستور نهادهای امنیتی، پیامک‌های فعال‌سازی را به راحتی بازپخش (SMS Interception) می‌کنند. حساب‌های خود را با شماره‌های ایرانی راه‌اندازی نکنید. و همیشه احراز هویت دو مرحله‌ای پیامکی را در تمام حساب‌ها خاموش کنید و آن را منحصراً روی اپلیکیشن‌های تولید توکن آفلاین مانند **Google Authenticator** یا **Aegis** تنظیم کنید.

- **فعال‌سازی پروتکل گذرکلید (Passkey):** در حساب‌های گوگل و پروتون‌میل، قابلیت Passkey را فعال کنید. این فناوری به جای رمز عبور، از سنسور اثر انگشت یا تشخیص چهره سخت‌افزاری گوشی شما برای ورود به حساب استفاده می‌کند و امکان لو رفتن رمز یا فیشینگ را به صفر می‌رساند.

- **قطع دسترسی به مخاطبین (Contacts Sync):** در تنظیمات حریم خصوصی تلگرام، گوگل و اینستاگرام، گزینه Sync Contacts را غیرفعال کرده و مخاطبین همگام‌سازی‌شده قبلی را حذف کنید (Delete Synced Contacts). این کار مانع از آن می‌شود که الگوریتم‌های سرکوب از طریق شماره تلفن‌های ذخیره‌شده در گوشی‌های مصادره‌شده، چارت ارتباطی هسته شما را ترسیم کنند.

نکته: در دنیای سایبر-فیزیکی، ابزارها به تنهایی معجزه نمی‌کنند؛ این «انضباط عملیاتی» و تکرار مداوم این پروتکل‌هاست که از شما یک کنشگر نفوذناپذیر می‌سازد. آگاهی شما، بالاترین سطح امنیت شماست.



5.4. سرویس ایمیل امن پروتون (ProtonMail)

ایمیل‌های سنتی (مانند Yahoo و Gmail) برای روزنامه‌نگاری شهروندی و ارسال اسناد حساس در مناطق پرخطر، بستری ناامن به شمار می‌روند؛ چرا که متادیتا را به طور کامل حفظ کرده و محتوای پیام‌ها روی سرورهای مرکزی به صورت متن ساده (Plain Text) قابل دسترسی و مانیتورینگ است. سرویس ProtonMail مستقر در سوئیس، استاندارد طلایی مکاتبات امن است که بر پایه معماری «دانش‌صفر» (Zero-Knowledge) و رمزنگاری سرتاسری (E2EE) بنا شده است؛ به این معنی که حتی خود شرکت پروتون نیز قادر به خواندن ایمیل‌های شما نیست.

پروتکل فعال‌سازی و راه‌اندازی حساب ایمیل امن

- **1.ثبت‌نام بدون ردپا:** هنگام ساخت حساب کاربری در پروتون‌میل، هرگز از ایمیل‌های قدیمی یا شماره تلفن شخصی خود برای تایید هویت (Verification) استفاده نکنید. برای عبور از سد تایید هویت، از گزینه‌هایی مثل پرداخت با رمزارزهای ناشناس (در صورت خرید نسخه پرمیوم) یا تایید از طریق کپچا (CAPTCHA) در بستر شبکه تور (Tor) استفاده کنید.
- **2.تنظیم گذرکلید (Passkey):** همان‌طور که در بخش‌های قبلی اشاره شد، برای مصون‌سازی حساب از فیشینگ و حملات هک رادیویی (برپایه سیم‌کارت)، رمز عبور سنتی را حذف کرده و ورود به اپلیکیشن پروتون را به ویژگی بیومتریک گوشی سخت‌افزاری خود (Passkey) متصل کنید.

تاکتیک‌های پیشرفته در زمان ارسال اسناد حساس

- **مکانیزم ایمیل‌های خودتخریب‌شونده (Self-Destructing Emails):** هنگام ارسال مدارک یا گزارش‌های نقض حقوق بشر به حساب‌های خارج از پروتون (یا حتی داخل شبکه)، قبل از زدن دکمه ارسال، روی آیکون ساعت کلیک کرده و یک تایمر (Expiration Time) (به طور مثال 24 یا 48 ساعت) تعیین کنید. با این کار، ایمیل پس از مدت زمان مشخص‌شده، به صورت خودکار و بدون بازگشت از صندوق ورودی گیرنده و فرستنده پاک خواهد شد.
- **ارسال پیام رمزگذاری‌شده به اکانت‌های غیرپروتون:** اگر مجبورید سندی را به یک ایمیل عادی (مثل جی‌میل یک سازمان یا رسانه) ارسال کنید، روی آیکون قفل در پایین منوی ارسال کلیک کنید و یک رمز عبور توافق‌شده برای ایمیل بگذارید. گیرنده تنها یک لینک دریافت می‌کند و برای باز کردن و دیدن محتوای ایمیل، باید رمز عبور را وارد کند. با این متد، فایروال‌های شبکه و شنودهای واسط، چیزی جز یک لینک رمزنگاری‌شده را مشاهده نخواهند کرد.
- **حذف خودکار متادیتای تصاویر پیوست:** پروتون‌میل به صورت خودکار برخی متادیتای پایه را در زمان ارسال ایمیل فیلتر می‌کند، اما طبق انضباط عملیاتی پروژه «صدای امن»، همواره باید فایل‌ها را ابتدا از طریق ابزارهایی مثل Scrambled Exif یا ExifCleaner پاک‌سازی کرده و سپس به ایمیل پیوست کنید.



سخن پایانی

کتابچه‌ای که ورق زدید و پروتکل‌هایی که مرور کردید، دستورالعمل‌هایی صرفاً برای حفاظت از داده‌ها نیستند؛ این ابزارها، جلیقه‌های ضدگلوله شما در جنگ پنهان سایبری هستند. در جغرافیای سختی چون اقلیم اهواز، هر تصویر، فیلم یا سندی که از نقض حقوق بشر ثبت و مخابره می‌شود، سنگی است که از دیوار بلند سانسور و بایکوت خبری فرو می‌ریزد. لنز دوربین شما، پنجره‌ای به سوی حقیقت است و برای باز نگه داشتن این پنجره، پنهان ماندنِ راوی یک اصل حیاتی است.

به یاد داشته باشید که امنیت یک وضعیت ایستا یا یک دکمه برای روشن کردن نیست؛ امنیت یک «انضباط مستمر و روزمره» است. ابزارها، اپلیکیشن‌ها و پروتکل‌های پیشرفته‌ای مانند شبکه پیازی، بریر، اوربسکوراکام و وراکریپت تنها زمانی معجزه می‌کنند که با وسواس عملیاتی، خونسردی و تکرار همیشگی همراه باشند. یک اشتباه کوچک یا یک لحظه غفلت ناشی از عجله در ارسال خبر، همان روزنه‌ای است که دستگاه سرکوب برای نفوذ به آن چشم دوخته است.

ما در این مسترکلاس آموختیم که چگونه دیوارهای سلول‌ها را شیشه‌ای کنیم، چگونه ردپای دیجیتال خود را از دید الگوریتم‌های پلیس فتا مخفی نگه داریم و چگونه در تاریکی مطلقِ قطع اینترنت، شریان ارتباطی جامعه مدنی را زنده بماند. اما فراتر از تکنولوژی، این «همبستگی، هوشیاری و آگاهی فنی» شماست که دژ نفوذناپذیر مقاومت را می‌سازد.

گمنام بمانید، نفوذناپذیر عمل کنید، جزئیات را با دقت فارنزیک پاک‌سازی کنید و به یاد داشته باشید که بزرگ‌ترین پیروزی در مستندسازی، روایتِ تمام‌عیار حقیقت است؛ به‌گونه‌ای که راوی برای روایت‌های بعدی زنده و آزاد بماند.



صـــدای امن

Secure Voice

sv.khro.org

info@khro.org