الدليل المرجعي الاحترافي لمقارنة برامج المراسلة الآمنة

(Telegram, Signal, Session)

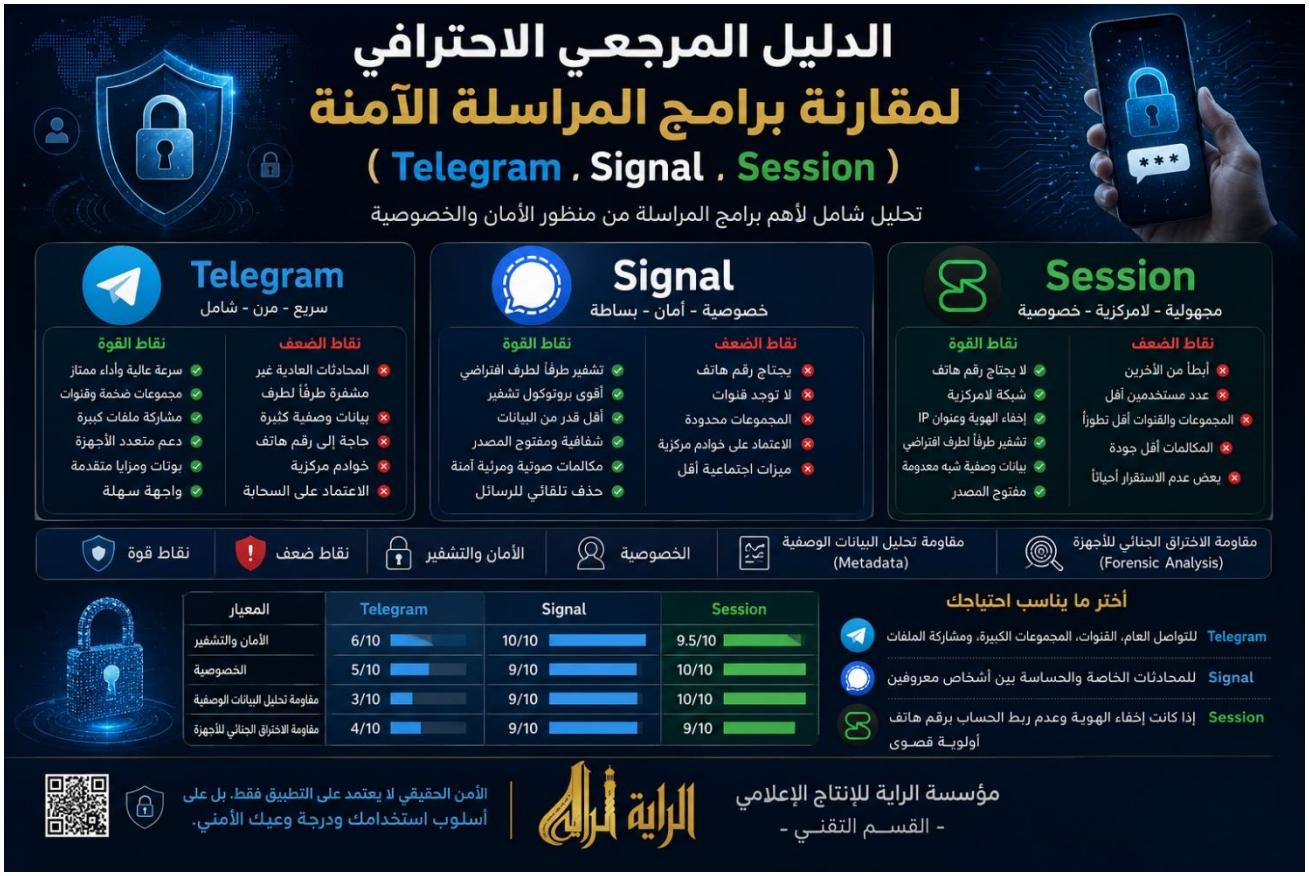
مُؤسَّسَةُ الرّاية لِلإِنْتَاجِ الإِعّلامِي

القِسْمُ التِّقْنّي

2026/07/30م

الدليل المرجعي الاحترافي لمقارنة برامج المراسلة الآمنة

(Telegram, Signal, Session)



أولاً: مقاومة تحليل البيانات الوصفية (Metadata):

البيانات الوصفية هي معلومات عن الاتصال، وليس محتوى الرسائل، مثل:

- من راسل من؟
- متى؟
- كم مرة؟
- مدة الاتصال.
- عنوان IP
- رقم الهاتف.
- جهات الاتصال.

- حجم الرسائل.

في كثير من الأحيان تكون هذه البيانات أهم من الرسائل نفسها بالنسبة لجهات التحقيق أو الاستخبارات.

1. تلغرام (Telegram): هو الأسوأ تقريباً حيث يحتفظ بقدر كبير من البيانات الوصفية مقارنةً بالآخرين، مثل:
   - رقم الهاتف.
   - عناوين IP لفترة.
   - الأجهزة المستخدمة.
   - جهات الاتصال إذا سمحت بالمزامنة.
   - معلومات الجلسات.

كما أن المحادثات العادية تمر بخوادمه المركزية وبالتالي يستطيع بناء خريطة اجتماعية (Social Graph) جيدة للمستخدمين.

2. سيجنال (Signal): صُمم لتقليل البيانات الوصفية قدر الإمكان وقد أضاف تقنية تسمى Sealed Sender، فحتى خادم Signal لا يعرف بسهولة من أرسل الرسالة إلى من في بعض الحالات كما أنه يحتفظ ببيانات قليلة جدًا عن الحساب لكن يبقى هناك:
   - رقم الهاتف.
   - بعض معلومات الاتصال بالشبكة.
   - إمكانية ملاحظة أن شخصًا ما يستخدم Signal.
3. سيشن (Session): هنا يتفوق لأنه:
   - لا يستخدم رقم هاتف.
   - لا يستخدم بريدًا إلكترونيًا.
   - يستخدم معرفًا عشوائيًا.
   - يمرر الرسائل عبر شبكة لامركزية متعددة العقد.
   - يخفي عنوان IP بدرجة كبيرة.

ولهذا يصعب جدًا رسم العلاقات بين المستخدمين.

ثانيًا: مقاومة الاختراق الجنائي للأجهزة (Forensic Analysis):

نفترض أن الجهاز نفسه أصبح في يد جهة متخصصة. ماذا ستجد؟

1. تلغرام (Telegram): إذا كان الهاتف مفتوحًا أو كان التطبيق مفتوحًا فقد تجد:
   - المحادثات.
   - الصور.
   - الملفات.
   - المجموعات.
   - القنوات.
   - أحيانًا إمكانية استعادة رسائل من السحابة بعد تسجيل الدخول إذا توفرت وسائل التحقق.

وبما أن المحادثات العادية مخزنة سحابيًا، فإن فقدان الجهاز ليس السيناريو الوحيد الذي يقلق المستخدم.

2. سيجنال (Signal): أفضل بكثير حيث يوفر:
   - تشفير قاعدة البيانات المحلية.
   - إمكانية قفل التطبيق.
   - حذف تلقائي للرسائل.
   - عدم وجود نسخة سحابية للمحادثات افتراضيًا.

لكن إذا كان الجهاز مفتوحًا بالفعل أثناء المصادرة، فسيظل الوصول إلى الرسائل ممكنًا.

3. سيشن (Session): مشابه ل Signal حيث يمتلك:
   - قاعدة بيانات محلية مشفرة.
   - عدم وجود نسخ سحابية تقليدية.

- حذف الرسائل المؤقتة.

لكن مثل أي تطبيق، إذا كان الجهاز مفتوحًا ومفكوك القفل وقت الاستيلاء عليه، فإن التشفير لا يمنع قراءة الرسائل المعروضة.

ثالثًا: الصمود أمام جهات استخبارات متقدمة:

وهنا يجب التفريق بين أمرين:

1. اعتراض الاتصالات عبر الشبكة.
2. اختراق جهاز المستخدم نفسه.

إذا تم اختراق الهاتف بزرع برمجية تجسس متقدمة، فلن يكون التطبيق وحده قادرًا على حماية الرسائل التي تُقرأ على الشاشة أو تُكتب عبر لوحة المفاتيح، مهما بلغت قوة التشفير.

أما إذا كان الحديث عن اعتراض الاتصالات فقط:

1. تلغرام (Telegram): إذا كانت المحادثة عادية:
   - تعتمد على خوادم Telegram
   - ليست مشفرة بين الطرفين فقط.

أما إذا كانت محادثة سرية (Secret Chat)، فيصبح اعتراض المحتوى أصعب بكثير، ومع ذلك، تبقى البيانات الوصفية والاعتماد على البنية المركزية عاملين مهمين.

2. سيجنال (Signal): يُعد من أكثر التطبيقات صمودًا في مواجهة اعتراض الاتصالات، بفضل بروتوكول Signal، والتشفير الطرفي الافتراضي، وتقليل البيانات الوصفية.
3. سيشن (Session): يضيف إلى التشفير مزايا إخفاء الهوية والبنية اللامركزية، ما يجعل الربط بين المستخدمين أكثر صعوبة، لكن الشبكة اللامركزية ليست ميزة مطلقة؛ فهي قد تؤثر على الأداء والاعتمادية مقارنةً بالبنية المركزية.

رابعاً: نقاط القوة والضعف:

1. تلغرام (Telegram):

- نقاط القوة:

- السرعة.
- المجموعات الضخمة (حتى مئات الآلاف).
- القنوات.
- مشاركة الملفات الكبيرة.
- تعدد الأجهزة.
- البوتات.
- البحث داخل الرسائل.
- التخزين السحابي.

ولهذا يستخدمه ملايين الأشخاص.

- نقاط الضعف:

- يحتاج رقم الهاتف؛ ورقم الهاتف يعتبر معرفًا قويًا لهويتك.
- الخوادم مركزية؛ أي أن Telegram يسيطر على كل البنية.
- يحتفظ بقدر كبير من البيانات الوصفية (Metadata) مقارنة بالآخرين.
- المحادثات العادية: وهنا يقع سوء الفهم عند كثير من الناس فهي ليست مشفرة End-to-End بل تكون:

Client ⇄ Telegram Server ⇄ Client

أي أن الرسالة تمر بخوادم Telegram بشكل يمكن للخدمة نفسها نظريًا فكها لأنها تعتمد تشفيرًا بين العميل والخادم وليس بين الطرفين فقط.

أما التشفير الكامل فلا يكون إلا في: المحادثة السرية (Secret Chats)، وهذه لها قيود:

- ❖ لا تعمل على عدة أجهزة.
- ❖ لا يوجد نسخ سحابي.
- ❖ لا يمكن استرجاعها.
- ❖ كثير من المستخدمين لا يستعملونها أصلاً.

2. سيجنال (Signal):

- نقاط القوة:

- جميع المحادثات مشفرة End-to-End من أول رسالة. لا تحتاج تفعيل شيء.
- بروتوكول Signal يعتبر أقوى بروتوكول تشفير مستخدم حاليًا، حتى أن تطبيقات كثيرة اعتمدته أو استوحت منه.
- أقل قدر من البيانات حيث أن Signal لا يحتفظ تقريبًا إلا بـ:
  - ❖ تاريخ إنشاء الحساب.
  - ❖ آخر اتصال تقريبًا.
  - ❖ ولا يحتفظ بقائمة الرسائل أو محتواها على الخادم.
- مفتوح المصدر؛ يمكن للباحثين مراجعة الكود.
- دعم ممتاز؛ يحصل على مراجعات أمنية مستمرة.
- قليل البيانات الوصفية (Metadata) حيث يستخدم تقنية Sealed Sender.

- نقاط الضعف:

- يحتاج رقم هاتف للتسجيل.
- يعتمد على خوادم مركزية.
- لا توجد قنوات مثل Telegram
- لا توجد مجموعات ضخمة جدًا.

3. سيشن (Session):

- نقاط القوة:

- لا يحتاج رقم هاتف ولا بريدًا إلكترونيًا، عند إنشاء الحساب تحصل على Session ID فقط وهذا وحده ميزة ضخمة.
- يعمل عبر شبكة لامركزية بدل وجود خادم واحد فتنتقل الرسائل عبر شبكة من العقد، وبالتالي يصعب جدًا ربط الرسائل بمكان واحد.
- يخفي عنوان IP بدرجة كبيرة، وهذا من أهم أهدافه.
- جميع الرسائل مشفرة End-to-End بشكل افتراضي.
- شبه انعدام البيانات الوصفية (Metadata).

- نقاط الضعف: بسبب الشبكة اللامركزية:
  - أبطأ من Telegram و Signal
  - أحيانًا يتأخر وصول الرسائل.
  - عدد المستخدمين أقل بكثير.
  - المكالمات الصوتية والفيديو ليست بنفس جودة المنافسين.

خامساً: من الأقوى في التشفير؟

1. Signal
2. Session
3. Telegram فقط في المحادثة السرية (Secret Chats).
4. Telegram العادي (الأضعف بينهم من ناحية الخصوصية).

سادساً: الأقوى في إخفاء الهوية؟

1. Session
2. Signal
3. Telegram

لأن:

- Session لا يطلب رقم هاتف.
- ويخفي الـ IP بدرجة أفضل.
- ويستخدم معرفًا عشوائيًا.

سابعاً: ماذا يوصي به خبراء الأمن؟

1. Session عندما تكون إخفاء الهوية أولوية قصوى.
2. Signal للتواصل الحساس.
3. Telegram للتواصل العام.

ثامناً: إذا كنت تعمل في بيئة عالية الخطورة:

- عدم استخدام Telegram للمعلومات الحساسة.

- استخدام Signal إذا كانت هوية الأطراف معروفة ولا يمانعون استخدام أرقام الهواتف.
- استخدام Session إذا كانت حماية الهوية وعدم ربط الحساب برقم هاتف أهم من سرعة الخدمة.

تاسعاً: بخصوص إنشاء قنوات أو مجموعات كبيرة:

مقارنة سريعة:

الميزة	Telegram	Signal	Session
مجموعات صغيرة	☆☆☆☆☆	☆☆☆☆☆	☆☆☆☆
مجموعات كبيرة	☆☆☆☆☆	☆☆☆	☆☆☆
قنوات نشر	ممتازة	لا	عبر Open Groups (بقدرات أقل)
إدارة آلاف الأعضاء	☆☆☆☆☆	☆☆	☆☆☆
البوتات	☆☆☆☆☆	لا	محدود جداً
مشاركة ملفات ضخمة	☆☆☆☆☆	☆☆☆	☆☆☆

عاشراً: الفتح في المتصفح (نسخة Web) ومزامنة سطح المكتب:

مقارنة سريعة:

الميزة	Telegram	Signal	Session
نسخة ويب تعمل داخل المتصفح	نعم	لا	لا
برنامج سطح المكتب	نعم	نعم	نعم
المزامنة بين الأجهزة	ممتازة	جيدة	جيدة (مع بعض القيود)

لماذا لا يقدم Signal و Session نسخة Web؟

السبب الرئيسي هو تقليل الهجوم (Attack Surface) حيث أن تطبيقات الويب تعتمد على المتصفح، والمتصفحات بيئات معقدة قد تتأثر بإضافات أو ثغرات أو جلسات عمل مشتركة. لذلك يفضّل مطورو Signal و Session الاعتماد على تطبيقات أصلية (Native Apps) للتحكم بشكل أفضل في مفاتيح التشفير والبيئة الأمنية.

أما Telegram فتعتمد تصميمًا مختلفًا يركز على سهولة الوصول من أي جهاز، مع الاعتماد على البنية السحابية، وهو ما يجعل نسخة الويب عملية جدًا، لكنه يأتي مع مفاضلات مختلفة في التصميم والخصوصية.

نقطة يغفل عنها كثير من الناس:

إذا تمكنت جهة متقدمة من الوصول إلى هاتفك وهو:

- مفتوح.
- أو غير محدث.
- أو مصاب ببرمجية تجسس.

فإن أقوى تشفير في العالم لن يمنعها من قراءة الرسائل أثناء استخدامها، لذلك يعتمد الأمن الحقيقي على مزيج من:

- تحديث نظام التشغيل.
- قفل الجهاز بكلمة مرور قوية.
- استخدام التشفير الكامل للجهاز.
- الحذر من الروابط والملفات غير الموثوقة.
- تفعيل القفل البيومتري أو برمز قوي للتطبيق إن كان متاحًا.

المقارنة المختصرة:

المعيار	Telegram	Signal	Session
التشفير الافتراضي	لا (في المحادثات العادية)	نعم	نعم
تشفير End-to-End	فقط Secret Chats	جميع الرسائل	جميع الرسائل
مفتوح المصدر	جزئياً	نعم	نعم
الخادم (Server)	مركزي	مركزي مع أقل قدر من البيانات	لامركزي
يحتاج رقم هاتف	نعم	نعم (يمكن إخفاءه لاحقا)	لا
يخزن بيانات على الخادم	نعم	أقل قدر ممكن	شبه معدوم
إخفاء الهوية	ضعيفة	جيدة	ممتازة
سهولة الاستخدام	ممتازة	ممتازة	جيدة
سرعة الرسائل	ممتازة	ممتازة	ضعيفة
القنوات	ممتازة	غير مدعومة	Open Groups
المجموعات الكبيرة	ممتازة	ضعيفة	جيد
حماية البيانات (Metadata)	ضعيفة	ممتازة	ممتازة
التوصية	للنشر العام	للتواصل الحساس	لإخفاء الهوية

خلاصة عملية

إذا أعطيت كل برنامج تقييمًا من 10:

الجانب	Telegram	Signal	Session
الأمان والتشفير	10/6 (Secret Chats 10/9)	10/10	10/9
الخصوصية	10/5	10/9	10/10
إخفاء الهوية	10/3	10/7	10/10
السرعة	10/10	10/9	10/7
سهولة الاستخدام	10/10	10/9	10/8
الاعتمادية	10/10	10/9	10/8
حماية البيانات الوصفية	10/3	10/9	10/10
مقاومة الاختراق	10/5 (Secret Chats 10/8)	10/9	10/9

هذا بافتراض أن الجهاز مقفل وسليم، أما إذا كان الجهاز مفتوحًا أو مخترقًا فإن مستوى الحماية ينخفض بغض النظر عن التطبيق.

توصيتي حسب السيناريو:

- Telegram: للتواصل اليومي العام، القنوات، المجموعات الكبيرة، ومشاركة الملفات، ونشر المحتوى، لكن لا تعتمد على محادثاته العادية للأمور الحساسة.
- Signal: هو الخيار الأقوى للتواصل الخاص والحساس من ناحية التشفير والتوازن بين الأمان وسهولة الاستخدام.
- Session: إذا كانت أولوية قصوى هي إخفاء الهوية وعدم ربط الحساب برقم هاتف أو تقليل إمكانية تتبع المستخدم، مع تقبل بعض التنازلات في السرعة والانتشار.

إعداد

القِسْمُ التِّقْنِّي

15 – صفر – 1448هـ.

2026/07/29م.