EN

A public-source case study

My independent public-source case study

TWO REAL CASES: A CYBER INCIDENT AND AN EARTHQUAKE

REAL SOURCES | SIMPLE ENGLISH | NO PRIVATE TARGETS

Personal work based only on public sources.

READ THIS FIRST

This booklet helps you explain a real method without saying more than you can prove.

Use only the sentences that are true for you.

I did not work for or represent any institution.

I used only public pages, reports and posts.

These are independent studies. They are not official casework.

BEFORE THE INTERVIEW

Open every source. Repeat the steps. Write your own notes. Then you can honestly say: “I reproduced this public-source comparison.”

The English and Turkish editions contain the same method and the same evidence limits.

STUDY CONTEXT

This is my independent public-source study

I chose two real cases to show how I check facts and limits.

WHAT THIS IS	WHAT THIS IS NOT
My own public-source research	Not work for an institution
Two real and checkable cases	No access to private systems
A method another person can repeat	No access to official case files

WHAT I SHOW

The two cases use the same five simple skills.

01 ASK

Start with one clear and limited question.

02 SAVE

Keep the source, date, time and exact wording.

03 COMPARE

Check the claim with another suitable source.

04 LIMIT

Write what the sources do not establish.

05 EXPLAIN

Make the method easy for another person to follow.

This is my own work based only on public information.

ADVANCED WORK CAN BE CLEAR AND SIMPLE

It starts with a clear question, careful source checks and clear limits.

Tools help find information. A method helps you check it.

QUESTION	SOURCE	CHECK	CONTEXT	LIMIT

MY THREE QUESTIONS

What exactly do I know?

How do I know it?

What is still missing?

A SIMPLE WAY OF WORKING

This order keeps the work clear and easy to review.

1. Keep the question clear and limited
2. Set authority and limits
3. Choose source types
4. Capture exact records
5. Check source and time
6. Compare explanations
7. Label each point as fact, assessment or unknown
8. Report, review, stop

If the legal purpose changes, go back to step 1.

A CLEAR QUESTION WITH LIMITS

A clear and limited question gives a clearer answer.

What can public Dutch sources show about the LAUNDRY BEAR incident of September 2024? What can they not show?

IN SCOPE	OUT OF SCOPE
Official public statements	Private people or accounts
One joint technical report	Protected systems or raw logs
Dates, wording and source chain	Attack testing or contact

STOP RULE

This demo stops at the public record of 27 May 2025.

KEEP A CLEAR RECORD OF WHERE EACH POINT CAME FROM

Provenance tells another reviewer where the information came from.

URL
Exact source address

TIME
Publication, access and time zone

WORDS
Exact wording before interpretation

VIEW
Screenshot or export under the rules

HASH
File fingerprint

NOTE
Change, limit and open question

REAL RECORD EXAMPLE R2

Source: politie.nl
Captured: 25 Aug 2026, 21:39 TRT
SHA-256 prefix: face2489c0680146f
Limit: the hash proves file identity, not the truth of the source claim.

TWO PAGES CAN USE THE SAME EVIDENCE

Check the information chain before calling it confirmation.

A **Original public record**

Official statement or technical report

B **Connected institution**

Useful for comparison. The sources may share evidence.

C **Secondary public report**

Useful for finding the original source

D **Repost or commentary**

A lead, not a second witness

Politie, AIVD and MIVD are consistent here, but they are connected institutional sources.

THREE LABELS KEEP THE WORDING ACCURATE

The label belongs to the sentence, not to the whole source.

REPORTED FACT

The public source directly reports or shows it.
“The Global Address List was taken.”

OFFICIAL ASSESSMENT

An authorised service states a conclusion with confidence language.
“The services assess it as very likely Russian state-sponsored.”

UNKNOWN

The sources in scope do not establish it.
Other stolen data: not established.

Important: “not established” does not mean “did not happen.”

PUBLIC INFORMATION STILL HAS LIMITS

In an authorised investigation, purpose, power, method and privacy impact matter.

NECESSARY?

Does the data answer the task?

PROPORTIONATE?

Does the intrusion fit the aim?

LESS INTRUSIVE?

Can I reach the aim with less data?

ACCURATE?

Did I separate fact and opinion?

STOP AND CONSULT

The purpose or authority is unclear.
The method enters a protected area.
The expected harm is higher than the value.
Sensitive data is not needed for the question.

Reference: Wet politiegegevens, Articles 3 and 4. This page is a work aid, not legal advice.

DO NOT TRUST YOUR FIRST EXPLANATION TOO QUICKLY

Good intentions do not remove bias.

FIRST STORY

The first explanation feels complete.

AUTHORITY EFFECT

An official source may make every detail feel certain.

CONFIRMATION BIAS

I search only for support.

URGENCY

Time pressure can hide weak wording.

Write one alternative explanation before you close the analysis.

In this case: “Russian state-sponsored” remains the services’ public assessment. This demo does not independently prove attribution.

LAUNDRY BEAR: HOW THE SOURCES ARE CONNECTED

Three public publications. One connected institutional evidence chain.

R2 POLITIE.NL

Impact and investigation

R3 AIVD.NL

Public assessment

LAUNDRY BEAR

PUBLIC INCIDENT CLAIMS

R4 AIVD AND MIVD

TLP:CLEAR report

I compare the wording, confidence level and limits. I do not repeat or test the attack.

EVENT TIME AND PUBLICATION TIME

Do not mix the day of the incident with the day of public disclosure.

23 SEP 2024 R4 p.1

The joint report gives the specific attack date.

SEP 2024 R2 AND R3

Politie and AIVD summaries refer to the incident month.

27 MAY 2025 R2, R3 AND R4

Politie statement, AIVD news and joint report are made public.

Same-day publication does not make the sources independent.

SOURCE 1 POLITIE

What the police page says

Read the exact public wording before adding interpretation.

REAL PUBLIC SOURCE

R2

ontwikkelingen. ‘Hoewel dit nieuws niet voor iedereen als een verrassing komt, kan het natuurlijk iets doen met je gevoel van veiligheid’, stelt zij daarin. ‘Uiteraard hebben we daar aandacht voor.’ De politie heeft daarom opnieuw een servicepunt ingericht waar medewerkers terecht kunnen met zorgen en vragen. De korpschef bedankte iedereen die een bijdrage leverde aan het onderzoek: ‘Jullie leverden een huzarenstukje.’

Impact

Bij de hack op de politie werd de Global Address List buitgemaakt. Daarin stonden de werkgerelateerde contactgegevens van politiemedewerkers en enkele ketenpartners. ‘De impact daarvan zowel op onze organisatie als de collega’s’, was groot’, vertelt Stan Duijf, hoofd Operatiën bij de eenheid Landelijke Opsporing en Interventies (LO), en verantwoordelijk voor cybercrime bij de politie. In stilte werden direct forse aanvullende beveiligingsmaatregelen genomen. Tegelijkertijd startte het Team High Tech Crime (THTC) een opsporingsonderzoek naar de daders. De uitkomsten daarvan ondersteunen de vandaag door de inlichtingendiensten gepubliceerde informatie. Daaruit blijkt dat de hackersgroep – die van de diensten de naam ‘LAUNDRY BEAR’ kreeg – cyberaanvallen uitvoerde op bedrijven en organisaties in ruim veertig westerse landen. Veel slachtoffers werden op een vrij generieke manier gemaakt. ‘De politie was één van de vele getroffen organisaties van deze hackersgroep’, zegt Duijf.

Feedback

politie.nl. Captured 25 Aug 2026 21:39 TRT. SHA-256 prefix: face2489. browser selection marks the sentence

SUPPORTS

The Global Address List was taken.
The page names the investigative and public context.

LIMIT

This page is a public statement, not the raw investigation file.

SOURCE 2 AIVD

The wording of uncertainty

The page gives a public assessment and a clear limit.

REAL PUBLIC SOURCE

R3

Home › Actueel › Nieuws

Onbekende Russische groep achter hacks Nederlandse doelen

Nieuwsbericht | 27-05-2025 | 11:00

Een tot nu toe onbekende Russische cybergroep zit achter de hacks op verschillende Nederlandse organisaties, waaronder de politie in september 2024. Bij de politie werden werkgerelateerde contactgegevens buitgemaakt. De diensten hebben niet kunnen vaststellen dat er ook andere gegevens zijn gestolen.

Dat blijkt uit onderzoek van de Nederlandse inlichtingen- en veiligheidsdiensten AIVD en MIVD. De diensten noemen de betrokken hackersgroep Laundry Bear. Inmiddels zijn de onderkende getroffen Nederlandse organisaties geïnformeerd. Ook zijn ze geholpen bij het nemen van maatregelen

aivd.nl. Captured 25 Aug 2026 21:40 TRT. SHA-256 prefix: e72a28a6. publication time is visible

SUPPORTS

The services publicly name LAUNDRY BEAR.
Work contact details were taken.
Other stolen data was not established.

LIMIT

“Not established” is an uncertainty statement. It is not proof that no other data was taken.

SOURCE 3 JOINT REPORT

Words such as “very likely” have a clear meaning

The report states its confidence level clearly.

REAL PUBLIC SOURCE

R4 P1

AIVD en MIVD onderkennen nieuwe Russische cyberactor

Dit is een gezamenlijke publicatie van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD). Een bijbehorend persbericht is gepubliceerd op de websites van de AIVD en het ministerie van Defensie.

1. **Samenvatting**

- De AIVD en MIVD hebben een tot nu toe publiek onbekende, zeer waarschijnlijk Russische staatsgesteunde cyberactor onderkend en de naam LAUNDRY BEAR gegeven.
- LAUNDRY BEAR is verantwoordelijk voor het uitvoeren van cyberoperaties tegen westerse overheden sinds 2024 en heeft een specifieke interesse in de krijgsmacht, overheden, defensie(toe)leveranciers, sociaal-maatschappelijke organisaties en digitale dienstverleners.
- Aanleiding voor het onderzoek naar deze actor was een opportunistische cyberaanval op de Nederlandse politie in september 2024. Bij deze aanval zijn werkgerelateerde contactgegevens van politiemedewerkers buitgemaakt. De diensten en de politie hebben niet kunnen vaststellen dat er andere gegevens zijn buitgemaakt. Zeer waarschijnlijk zijn ook andere Nederlandse organisaties slachtoffer geweest van deze actor.
- LAUNDRY BEAR weet onder de radar te blijven door gebruik te maken van eenvoudige aanvalstechnieken en -paden die beschikbaar zijn op de computer van een slachtoffer, die lastig te detecteren zijn voor organisaties en lastig te onderscheiden zijn van andere bekende Russische actoren.

2. **Oorsprong en attributie**

Op 23 september 2024 werd de politie slachtoffer van een cyberaanval waarbij de werkgerelateerde contactgegevens van alle politiemedewerkers door een cyberactor zijn buitgemaakt. Uit daaropvolgend technisch onderzoek van de diensten is gebleken dat deze cyberaanval is uitgevoerd door een tot nu onbekend gebleven, zeer waarschijnlijk

AIVD and MIVD technical report. Captured 25 Aug 2026 21:40 TRT. SHA-256 prefix: 4903906d. fixed reading crop

SUPPORTS

Specific incident date: 23 September 2024.
“Very likely” marks the attribution confidence.
The report says its view is not complete.

LIMIT

This is an official public assessment. The demo cannot inspect the classified or raw evidence behind it.

SOURCE 3 TECHNICAL DETAIL

Useful detail, clear boundary

The report explains the assessed path at a public defensive level.

REAL PUBLIC SOURCE R4 P3

2.1.3 ***Ook Nederlandse slachtoffers***

In september 2024 verkreeg LAUNDRY BEAR toegang tot een account van een medewerker van de Nederlandse politie. Hierbij is het de actor gelukt om via dit account de werkgerelateerde contactgegevens – de GAL – van politiemedewerkers buit te maken. Uit technisch onderzoek blijkt dat de actor zeer waarschijnlijk de politie opportunistisch heeft aangevallen via een *pass-the-cookieaanval*.[3] Dit is een techniek waarbij de actor zich voordoet als de eigenaar van een cookie. Naar aanleiding van het technische onderzoek achten de diensten het waarschijnlijk dat deze cookie is buitgemaakt via *infostealer*-malware van mogelijk een derde partij en daarna door LAUNDRY BEAR via criminele fora is aangeschaft. Met deze buitgemaakte cookie kan de actor zonder een wachtwoord of gebruikersnaam in te vullen toegang verkrijgen tot bepaalde informatie.

De diensten en de politie hebben niet kunnen vaststellen dat er door LAUNDRY BEAR via dit account andere gegevens dan de GAL zijn buitgemaakt. Technisch onderzoek wijst uit dat LAUNDRY BEAR zeer waarschijnlijk ook andere Nederlandse slachtoffers heeft gemaakt.

2.2 Impact van techniek op snelheid en succesvolle aanvallen

AIVD and MIVD technical report. Captured 25 Aug 2026 21:40 TRT. SHA-256 prefix: 4903906d. page 3 reading crop

SUPPORTS

The report describes assessed account access and the GAL result.
It repeats the limit on other data.
It gives enough context to compare sources.

LIMIT

I do not turn a defensive public report into attack instructions or test any real system.

THE EVIDENCE MATRIX

YES means the public source says it. It does not mean I saw the underlying case evidence.

CLAIM	R2	R3	R4	LABEL
September 2024 incident	YES	YES	YES	reported
Work contacts and the GAL were taken	YES	YES	YES	reported
Very likely Russian state-sponsored	INDIRECT	YES	YES	assessment
Other data taken	NOT STATED	NOT SHOWN	NOT SHOWN	unknown
Full technical chain proven here	NO	NO	NO	not shown

Conclusion: the public record supports the incident and the institutional assessment. It does not independently reproduce attribution.

WHAT I CHECKED AND WHAT REMAINS UNPROVEN

A strong interview answer includes both sides.

I DID	I DID NOT
Defined one public question	Target a private person
Captured official sources	Access any protected system
Recorded dates, URLs and hashes	Inspect confidential case evidence
Compared exact wording	Independently attribute the actor
Marked assessment and unknowns	Invent an interview or result

This is my independent public-source comparison. I did not use protected systems or case files.

Say “I did” only after you personally repeat the source checks.

SIMPLE ANSWERS YOU CAN USE IF THEY ARE TRUE FOR YOU

Keep the words simple. Add only your real experience.

WHY THIS STUDY?

“I wanted to show how I turn public information into a clear and traceable result.”

HOW DO YOU WORK?

“I keep the question clear, record the source, compare explanations and separate facts, assessments and unknowns.”

WHAT IS YOUR EXPERIENCE?

“One real example is [project]. My task was [task]. I checked [sources], recorded [evidence] and reached [real result].”

WHAT UNDER PRESSURE?

“I protect the basic checks. If time is short, I reduce scope. I do not hide uncertainty.”

WHAT IF YOU DO NOT KNOW?

“I say what is missing, search one more suitable source and ask for legal or technical review when needed.”

If you need to answer in English: “Mijn Nederlands is in ontwikkeling. Mag ik dit technische antwoord in eenvoudig Engels geven?”

A SIMPLE STAR EXAMPLE AND THE SOURCES

Use the STAR only after you repeat the demo yourself.

Situation: I reviewed public Dutch statements about LAUNDRY BEAR.
Task: I separated reported facts, official assessments and unknowns.
Action: I made a source log, timeline and evidence matrix.
Result: I wrote a short conclusion with clear limits and checkable links.

THREE QUESTIONS I CAN ASK IN AN INTERVIEW

How does the team review source quality and reporting?

How are legal or privacy doubts escalated?

What should success look like in the first six months?

SOURCES CHECKED ON 25 AUG 2026

S1	Politie: public incident update
S2	AIVD: public LAUNDRY BEAR statement
S3	AIVD and MIVD report on Defensie
S4	Wet politiegegevens, Articles 3-4
S5	NIST IR 8387: evidence preservation
S6	Wason 1960: confirmation bias

Write only what the sources support. State what is missing.

CASE 2 CHECKING INFORMATION DURING A CRISIS

How I checked a real public post

The account posts in English. I check the event against official public sources.

I use the post as a starting point, not as proof.

S1 PUBLIC POST

@USGS_Quakes

S2 ACCOUNT OWNER

usgs.gov

S3 EVENT RECORD

us7000rm3k

S4 OTHER INSTITUTE

UNAM

WHAT THIS CHECK SHOWS

I check who owns the account.

I connect the post to a stable event number.

I compare the facts with a second institution.

I do not use private accounts or hidden data.

METHOD

A simple seven-step check

Another person can follow and check each step.

1. Write one question.
2. Save the post URL and visible content.
3. Check who owns the account.
4. Find the stable event record.
5. Compare one independent institution.
6. Record facts, limits and changed values.
7. Write what remains unknown.

I stop if the task needs private data, direct contact, a login or more legal authority.

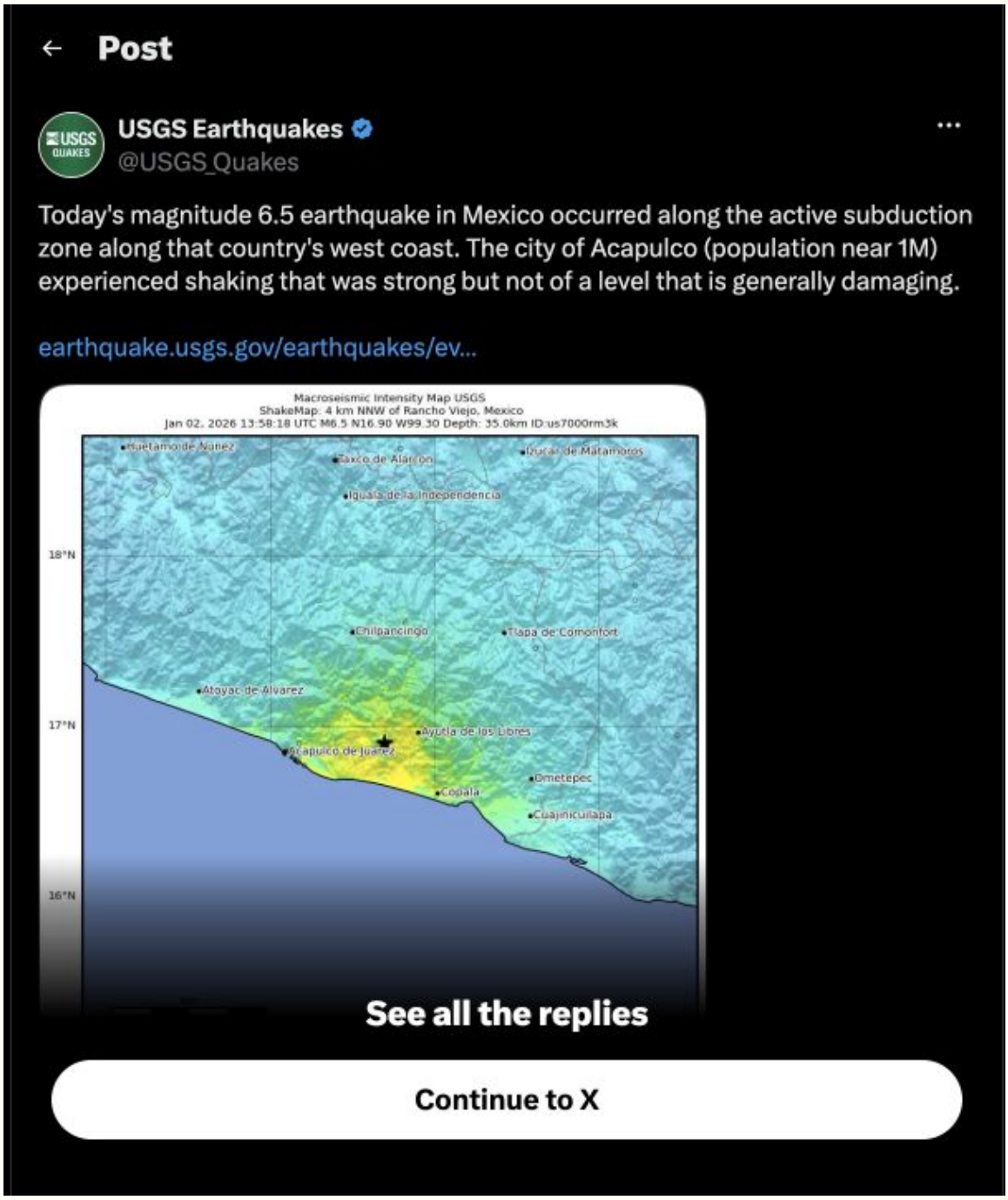
SOCMINT SOURCE 1 PUBLIC POST

Save the original post

I save the source before I add my own view.

REAL PUBLIC SOURCE

S1



@USGS_Quakes on X. Captured 25 Aug 2026 21:55 TRT. SHA-256 prefix: 49c0582e. fixed reading crop

SUPPORTS

The account name, handle and public claim are visible.
The post links to an earthquake record.

LIMIT

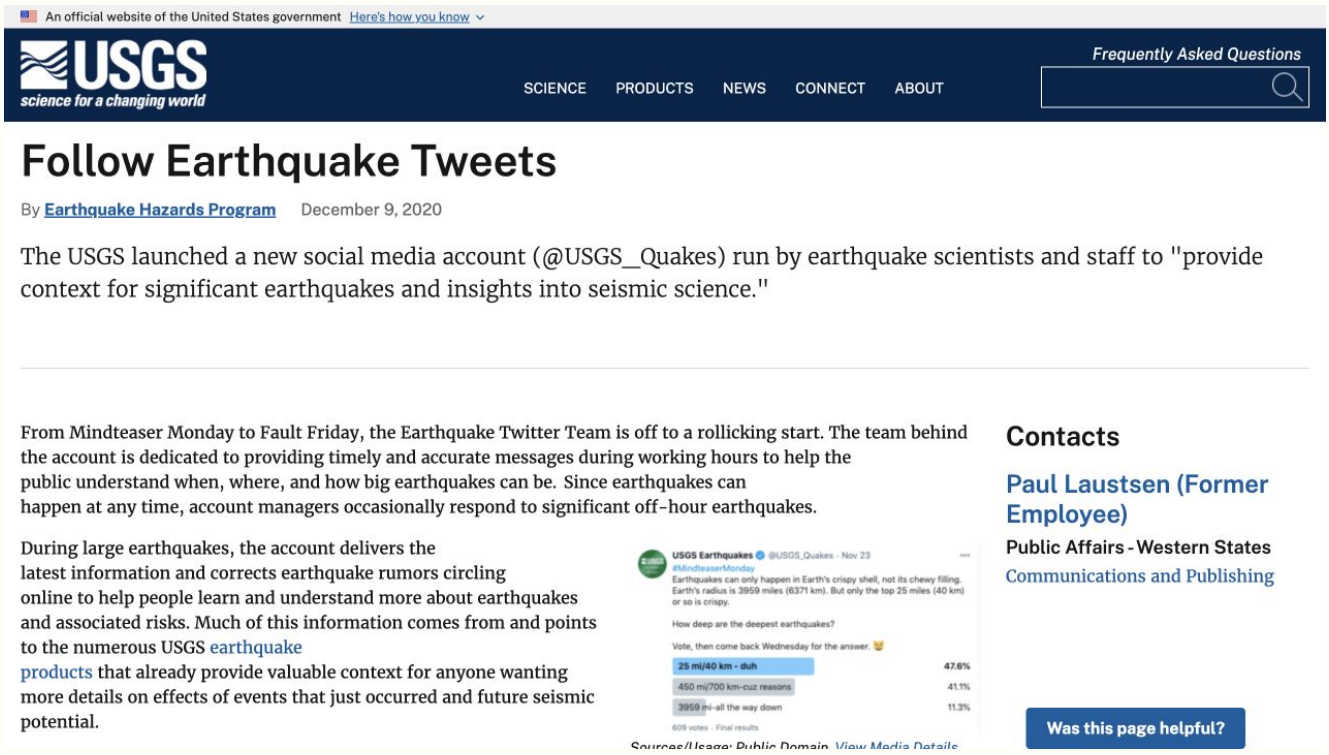
The post alone does not prove account ownership, final event values or damage.

SOCMINT SOURCE 2 ACCOUNT OWNER

Verify the account on usgs.gov

I use the institution's own website, not only the platform badge.

REAL PUBLIC SOURCE S2



usgs.gov. Captured 25 Aug 2026 21:56 TRT. SHA-256 prefix: fa89cf5d. official ownership statement

SUPPORTS

USGS says @USGS_Quakes is run by its scientists and staff.
The page explains the account's public-information role.

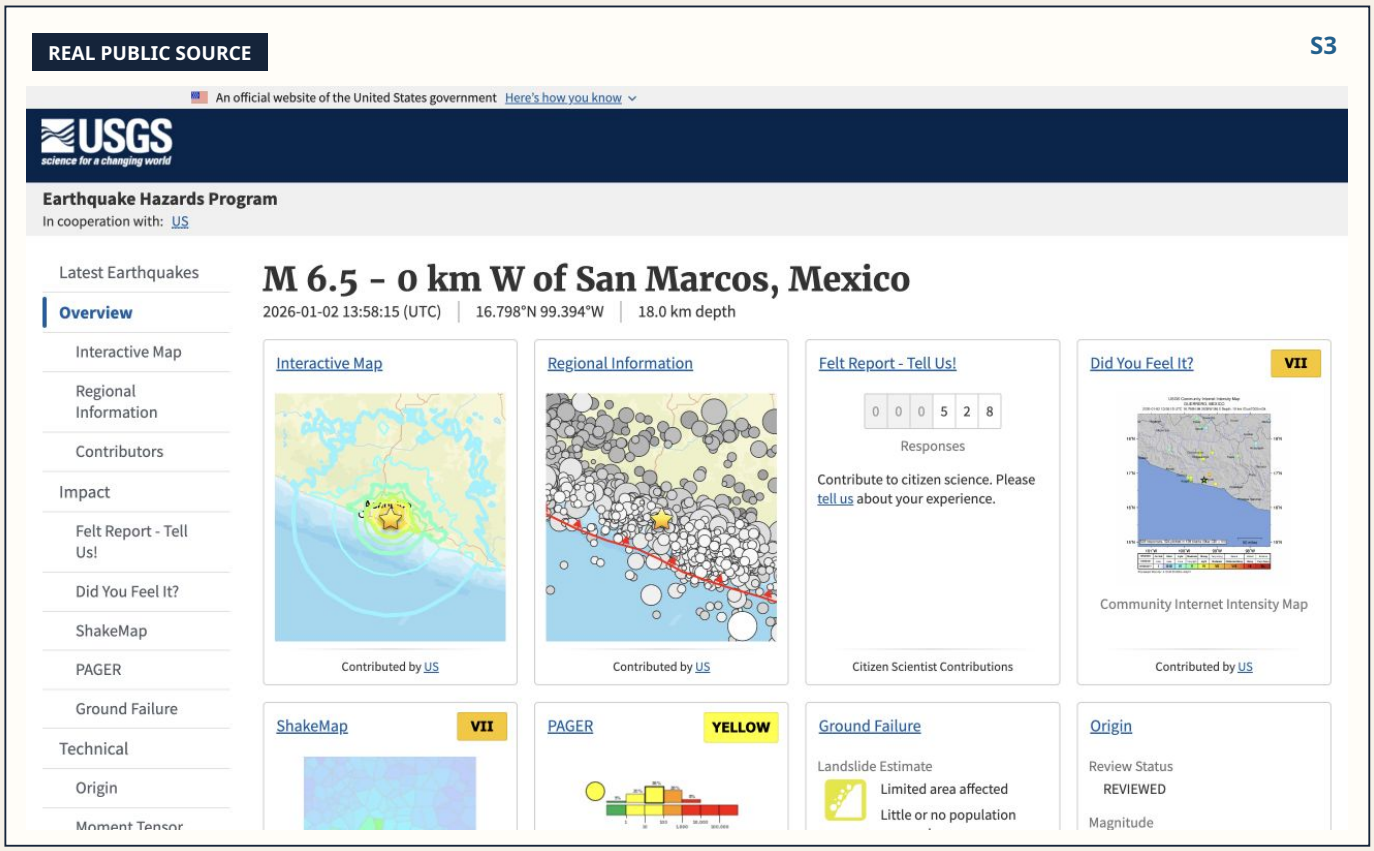
LIMIT

An official account can still publish early or incomplete information.

SOCMINT SOURCE 3 EVENT RECORD

Match the post to us7000rm3k

The event number gives me a stable record to check.



USGS event us7000rm3k. Captured 25 Aug 2026 21:56 TRT. SHA-256 prefix: 7b7f339a. reviewed event page

SUPPORTS

Magnitude 6.5 west of San Marcos, Mexico.
2 January 2026 at 13:58:15 UTC. Status: reviewed.
Event number: us7000rm3k.

LIMIT

The record can be updated. Record the version and time you checked it.

SOCMINT SOURCE 4 INDEPENDENT CHECK

Check an independent source

UNAM gives a separate scientific record of the same event.

REAL PUBLIC SOURCE S4 P1

2026/01/05: Reporte rápido del Servicio Mareográfico Nacional del Instituto de Geofísica de la Universidad Nacional Autónoma de México

Registro del tsunami en la estación mareográfica de Acapulco del Servicio Mareográfico Nacional por el sismo de magnitud 6.5 ocurrido el 2 de enero de 2026

RESUMEN

El día 2 de enero de 2026 se registró un pequeño tsunami en la estación mareográfica de Acapulco, producto de un sismo de magnitud 6.5, ocurrido a las 7:58 hora del Centro de México (13:58 UTC), el cual se ubicó a una profundidad de 5 km, y su epicentro se localizó en la latitud: 16.77° y en la longitud: -99.413°, en las cercanías de San Marcos, Guerrero.

El Servicio Mareográfico Nacional, operado por el Instituto de Geofísica de la Universidad Nacional Autónoma de México, quien mantiene un monitoreo permanente del nivel del mar en las costas de México, inició su protocolo de vigilancia ante la ocurrencia de un posible tsunami.

La estación que registró la llegada de las ondas del tsunami fue la estación de Acapulco, 14 minutos después de la ocurrencia del sismo. La amplitud máxima de pico a pico registrada fue de 9.62 cm.

UNAM technical report. Captured 25 Aug 2026 21:57 TRT. SHA-256 prefix: 24ad9213. page 1 reading crop

SUPPORTS

A real M6.5 earthquake on 2 January 2026.
The report places it near San Marcos, Guerrero.
It records a small tsunami signal at Acapulco.

LIMIT

This report is in Spanish. Translate carefully and keep the original wording available.

CHECK RESULT

What the check shows and does not show

I keep confirmed points and missing points separate.

CONFIRMED	NOT SHOWN
USGS says its team runs the account	The full amount of damage
USGS has a reviewed M6.5 event record	Every injury or damage claim
The time and area match the post	Who saw or believed the post
UNAM records the same earthquake	Information about private people

SIMPLE REPORT WORDING

USGS states that it runs the account. The public records confirm the earthquake. They do not show its full effect. I would record this limit and wait for more information.

If the numbers change, I record the source, version and time. I do not call a source false without evidence.

ONE-MINUTE ANSWER

My one-minute answer

I only say what I checked myself.

> “I used a real public post from @USGS_Quakes. First, I checked on usgs.gov that the account is run by USGS staff. Next, I matched the post with event us7000rm3k. Then I used a UNAM report as a separate check. The sources confirm a magnitude 6.5 earthquake near San Marcos on 2 January 2026. They do not show the full damage. I wrote that limit clearly.”

CASE SOURCES CHECKED ON 25 AUG 2026

S1	@USGS_Quakes public X post
S2	USGS official account page
S3	USGS reviewed event us7000rm3k
S4	UNAM public technical report

Use this only after you repeat the checks. This is my independent interview practice. It is not an official investigation.