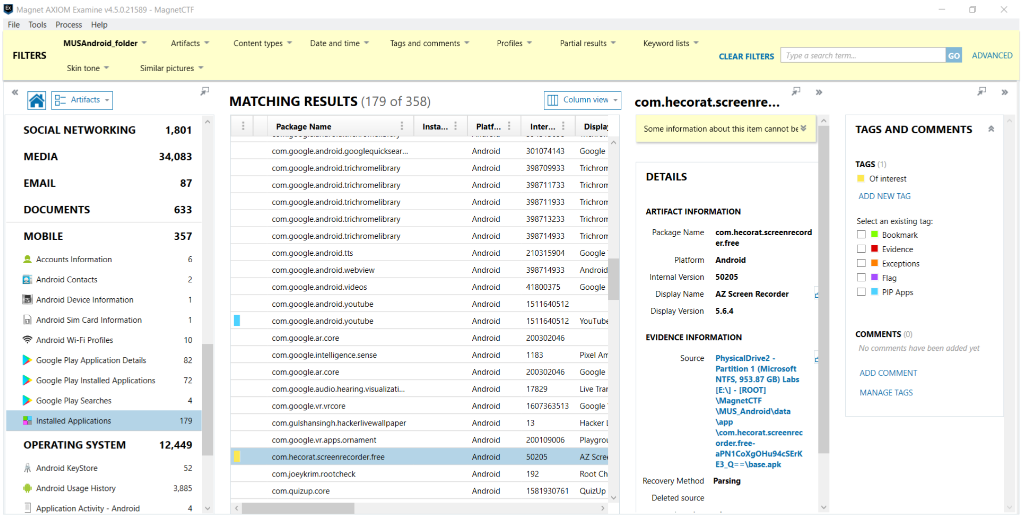
Magnet CTF:

Question 2 Solution Walk-Through

Challenge 2 (OCT 12-18) PIP Install: What domain was most recently viewed via an app that has picture-in-picture capability?

For the week 2 challenge, we're using the same Android image we examined last week. From the question there's two factors involved, application capability and application usage.

The first thing to understand is what applications on the device have PIP (Picture in Picture) capability.



SOCIAL NETWORKING	1,801
MEDIA	34,083
EMAIL	87
DOCUMENTS	633
MOBILE	357
Accounts Information	6
Android Contacts	2
Android Device Information	1
Android Sim Card Information	1
Android Wi-Fi Profiles	10
Google Play Application Details	82
Google Play Installed Applications	72
Google Play Searches	4
Installed Applications	179
OPERATING SYSTEM	12,449
Android KeyStore	52
Android Usage History	3,885
Application Activity - Android	4

MATCHING RESULTS (179 of 358)

	Package Name	Insta...	Platf...	Inter...	Displa
	com.google.android.googlequicksear...		Android	301074143	Google
	com.google.android.trichromelibrary		Android	398709933	Trichron
	com.google.android.trichromelibrary		Android	398711733	Trichron
	com.google.android.trichromelibrary		Android	398711933	Trichron
	com.google.android.trichromelibrary		Android	398713233	Trichron
	com.google.android.trichromelibrary		Android	398714933	Trichron
	com.google.android.tts		Android	210315904	Google
	com.google.android.webview		Android	398714933	Android
	com.google.android.videos		Android	41800375	Google
	com.google.android.youtube		Android	1511640512	
🟦	com.google.android.youtube		Android	1511640512	YouTube
	com.google.ar.core		Android	200302046	
	com.google.intelligence.sense		Android	1183	Pixel Am
	com.google.ar.core		Android	200302046	Google
	com.google.audio.hearing.visualizati...		Android	17829	Live Trar
	com.google.vr.vrcore		Android	1607363513	Google
	com.gulshansingh.hackerlivewallpaper		Android	13	Hacker L
	com.google.vr.apps.ornament		Android	200109006	Playgrou
🟨	com.hecorat.screenrecorder.free		Android	50205	AZ Scre
	com.joeykrim.rootcheck		Android	192	Root Ch
	com.quizup.core		Android	1581930761	QuizUp

com.hecorat.screenre...

Some information about this item cannot be

DETAILS

ARTIFACT INFORMATION

Package Name	com.hecorat.screenrecorder.free
Platform	Android
Internal Version	50205
Display Name	AZ Screen Recorder
Display Version	5.6.4

EVIDENCE INFORMATION

Source	PhysicalDrive2 - Partition 1 (Microsoft NTFS, 953.87 GB) Labs [E:\] - [ROOT] \MagnetCTF \MUS_Android\data \app \com.hecorat.screenrecorder.free-aPN1CoXgOHu94cSErKE3_Q==\base.apk
Recovery Method	Parsing
Deleted source	

TAGS AND COMMENTS

TAGS (1)

🟨 Of interest

ADD NEW TAG

Select an existing tag:

- ☐ 🟩 Bookmark
- ☐ 🟥 Evidence
- ☐ 🟧 Exceptions
- ☐ 🟪 Flag
- ☐ 🟦 PIP Apps

COMMENTS (0)

No comments have been added yet

ADD COMMENT

MANAGE TAGS

Time zone UTC+0:00

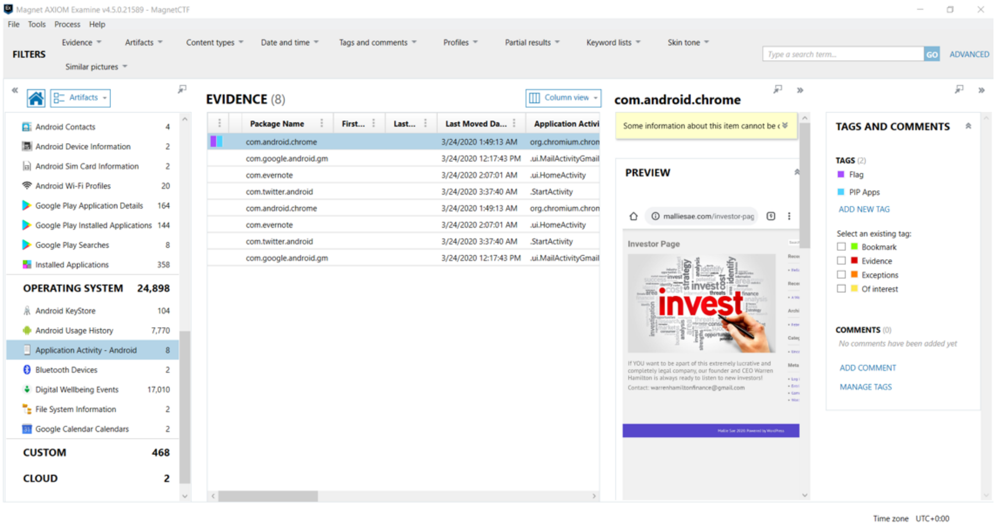
I reviewed the installed applications on the device looking for anything that could be PIP related. A screen recording application caught my attention (googled to understand capability), but this was not the 'Droid (app) we're looking for.

One of the Discord users shared this helpful link describing the capability and what applications featured PIP support.

https://nokiapoweruser.com/list-apps-support-oreo-picture-picture-mode-enable/

Back to the applications I tagged anything listed that showed up in the PIP article.

From here I proceeded to look at the **Application Activity – Android.** One of the applications we can see recent activity for is Google Chrome. From the previously referenced article we know this app supports PIP.



Android Contacts	4
Android Device Information	2
Android Sim Card Information	2
Android Wi-Fi Profiles	20
Google Play Application Details	164
Google Play Installed Applications	144
Google Play Searches	8
Installed Applications	358
OPERATING SYSTEM	**24,898**
Android KeyStore	104
Android Usage History	7,770
Application Activity - Android	8
Bluetooth Devices	2
Digital Wellbeing Events	17,010
File System Information	2
Google Calendar Calendars	2
CUSTOM	**468**
CLOUD	**2**

EVIDENCE (8)

Package Name	First...	Last...	Last Moved Da...	Application Activi
com.android.chrome			3/24/2020 1:49:13 AM	org.chromium.chron
com.google.android.gm			3/24/2020 12:17:43 PM	.ui.MailActivityGmail
com.evernote			3/24/2020 2:07:01 AM	.ui.HomeActivity
com.twitter.android			3/24/2020 3:37:40 AM	.StartActivity
com.android.chrome			3/24/2020 1:49:13 AM	org.chromium.chron
com.evernote			3/24/2020 2:07:01 AM	.ui.HomeActivity
com.twitter.android			3/24/2020 3:37:40 AM	.StartActivity
com.google.android.gm			3/24/2020 12:17:43 PM	.ui.MailActivityGmail

com.android.chrome

Some information about this item cannot be d

PREVIEW

malliesae.com/investor-pag

Investor Page

If YOU want to be apart of this extremely lucrative and completely legal company, our founder and CEO Warren Hamilton is always ready to listen to new investors!

Contact: warrenhamiltonfinance@gmail.com

TAGS (2)

- Flag
- PIP Apps

Select an existing tag:

- □ Bookmark
- □ Evidence
- □ Exceptions
- □ Of interest

COMMENTS (0)

No comments have been added yet

Time zone UTC+0:00

In the preview card we can see that it was captured that Chrome was used to visit a URL beginning with **MallieSae.com.**

The artifact for this can be found at **MUS_Android.tar\data\system_ce\0\snapshots\320.jpg**

Answer: Google Chrome, an app that supports PIP, was recently used visit the domain **malliesae.com**