

لیست آزمون‌های سایبری دوربین‌های مدار بسته در آزمایشگاه سامانه‌های الکترونیکی و هوشمند جهاد دانشگاهی صنعتی شریف

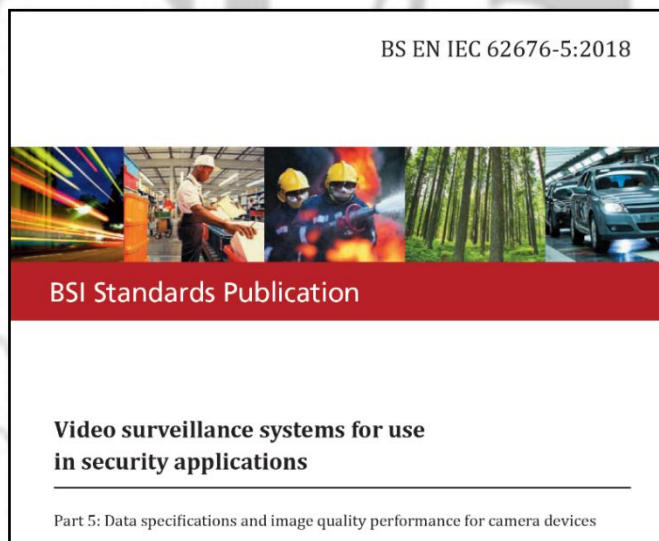
آزمون‌های سایبری دوربین مدار بسته در دو دسته زیر قرار می‌گیرند:

۱. آزمون‌های کیفیت تصویر (استریم) دوربین

۲. آزمون‌های تست نفوذ دوربین

آزمون رزولوشن (تفکیک‌پذیری):

قبل از پرداختن به روش انجام این آزمون لازم است ابتدا به تعریف این واژه مطابق استاندارد IEC 62676-5 بپردازیم. این استاندارد جامع‌ترین استاندارد بین‌المللی در زمینه ارزیابی عملکرد سامانه‌های نظارت تصویری است.



تصویر ۱: استاندارد IEC 62676

مطابق این استاندارد دو تعریف برای واژه Resolution مطابق تصویر زیر تعریف شده است؛

3.1.65

resolution

<related to visual resolution> measure of the ability of a camera or video systems to reproduce detail from the original scene or image

3.1.66

resolution

<related to format> description of the size of a digital image in pixels (e.g. 720P, 1080P, 640 × 480), pixels per inch or number of pixels of a video-frame, monitoring device, printout

تصویر ۲: تعاریف واژه Resolution

تعریف نخست، بیانگر توانایی دوربین در ثبت جزئیات صحنه و تعریف دوم برای بیان سائز تصویر به پیکسل است.

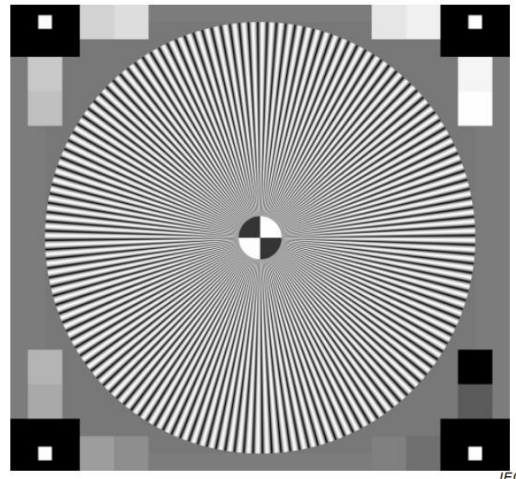
برای رزولوشن به معنای دوم (سائز تصویر به پیکسل) روش آزمونی در استاندارد بیان نشده است و به صورت نرم افزاری این امکان در برنامه‌نویسی firmware دوربین فراهم است که ابعاد تصویر را upsample کرده و به بیانی مگاپیکسل بزرگتری را خروج دهد.

حال آنکه برای تعریف نخست واژه رزولوشن (resolving power)، توانایی دوربین در ثبت جزئیات، روش آزمونی مطابق زیر معرفی شده است.

5	Measurement methods of video surveillance camera specification items	41
5.1	Setting of standard shooting condition	41
5.1.1	General	41
5.1.2	Common standard shooting condition	42
5.2	Video signal quantization level	44
5.2.1	General	44
5.2.2	Digital video signal quantization level	44
5.2.3	Other quantization levels	44
5.3	Measurement environment	44
5.3.1	General	44
5.3.2	Test chart	45
5.3.3	Software for measurement	48
5.4	Measuring methods	48
5.4.1	General	48
5.4.2	Resolution	48
5.4.3	Minimum illumination	56
5.4.4	Dynamic range	59
5.4.5	Visible dynamic range (VDR)	67
5.4.6	Infra-red illumination operating view distance	70
5.4.7	Image distortion	73
5.4.8	Image flare	77
5.4.9	Capture frame rate	84

تصویر ۳: استاندارد IEC 62676

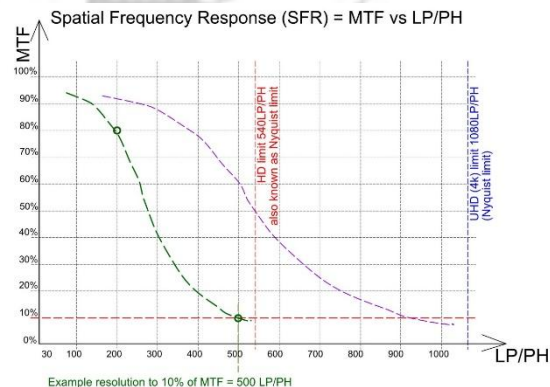
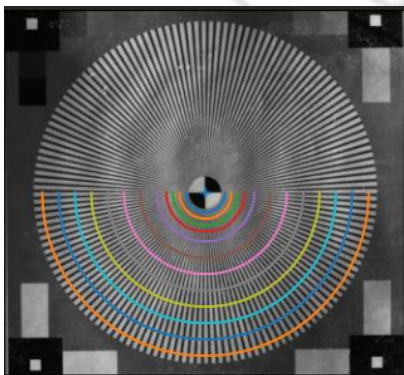
برای انجام آزمون تست چارتری مطابق تصویر زیر ارائه شده است که به Sinusoidal Siemens Star معروف است. در تست چارت هر چه به مرکز تصویر حرکت می‌کنیم، فرکانس فضایی (Spatial Frequency) افزایش می‌یابد و توانایی دوربین را در ثبت جزئیات ارزیابی می‌کند.



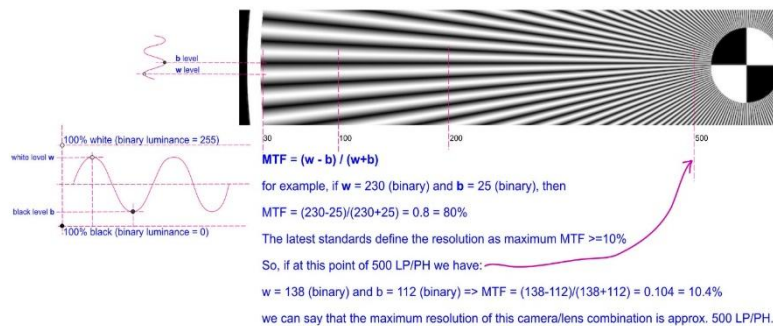
تصویر ۴: تست چارت

ابتدا در شرایط آزمون و در اتاق تاریک توسط دوربین مدار بسته یک تصویر از تست چارت می‌گیریم و سپس آن را برای تحلیل به نرم‌افزار می‌دهیم؛ روش اندازه‌گیری به این صورت است که هر چه به سمت مرکز تصویر حرکت کنیم، از جایی (فرکانس فضایی) که قادر به تفکیک خطوط سیاه و سفید نباشیم آن فرکانس در گزارش آزمون ماکسیمم رزولوشن گزارش می‌شود. اگر شما به تست چارت اصلی (تست چارتی که توسط پرینترهای تخصصی و روی کاغذهای خاص پرینت گرفته شده باشد که متاسفانه تکنولوژی پرینت آن تنها در اختیار کشور آمریکا است و از هم تست چارت و هم نرم‌افزار از کمپانی اصلی سازنده تهیه شده است.) با چشم دقت کنید، از آنجایی که چشم انسان قدرت تفکیک پذیری بسیار بالایی دارد، حتی در مرکز تست چارت نیز قادر به تفکیک خطوط سیاه و سفید از یکدیگر هستید؛ اما با توجه به توانایی هر دوربین در ثبت جزئیات، فرکانس‌های متفاوتی گزارش می‌شوند؛

به عنوان نمونه آزمون رزولوشن یک دوربین مدار بسته انجام شده را در تصویر زیر مشاهده می‌کنید که به ازای تمام دواير متحد المركز صورت می‌گیرد.



تصویر ۵: گزارش آزمون SFR



تصویر ۶: روش انجام آزمون

به همین علت هم هست که اگر دو دوربین ۸ و ۴ مگاپیکسلی را از نظر رزولوشن (به معنای قدرت تفکیک پذیری) بررسی کنیم، ممکن است دوربین ۴ مگاپیکسلی قادر به ثبت جزئیات و تفکیک پذیری بالایی باشد (به بیانی دیگر شیب میرایی منحنی آن کمتر از شیب میرایی دوربین ۸ مگاپیکسلی باشد).

این اشتباه در بیان کیفیت تصویر با واژه مگاپیکسل (Pixel Count) و تفاوت آن با واژه Resolution در بخش Technical Background استاندارد ISO 12233:2023 (که خود مرجع IEC 62676 است) بیان شده است.



تصویر ۸: استاندارد ISO 12233

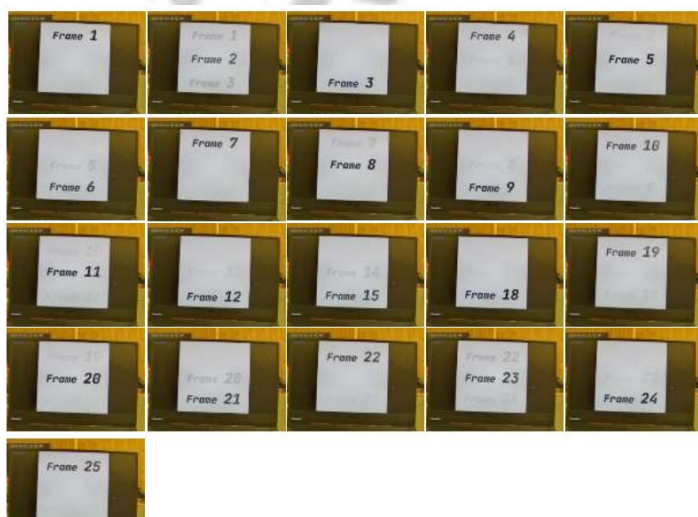
Technical background

Because digital cameras are sampled imaging systems, the term *resolution* is often incorrectly interpreted as the number of addressable photoelements. While there are existing protocols for determining camera pixel counts, these are not to be confused with the interpretation of resolution as addressed in this document. Qualitatively, resolution is the ability of a camera to optically capture finely spaced detail, and is usually reported as a single valued metric. Spatial frequency response (SFR) is a

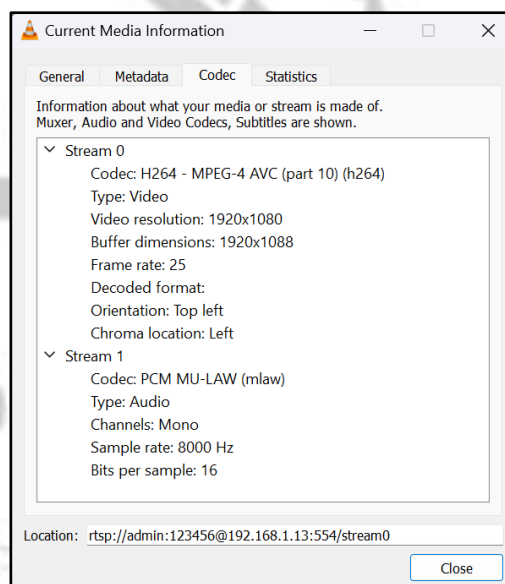
تصویر ۷: استاندارد ISO 12233

آزمون نرخ حقیقی فریم (Frame Rate) دوربین:

نرخ فریم دوربین بیانگر تعداد فریم نمایش داده شده در یک ثانیه از استریم است؛ از آنجایی که نرخ فریم بالاتر به دوربین ب مشخصات بهتری نیاز است، در نتیجه تعدادی از تولیدکنندگان اقدام به افزایش ظاهری نرخ فریم در firmware دوربین می‌کنند (به عنوان مثال هر فریم را به صورت نرم افزاری duplicate کرده و نمایش می‌دهند)؛ با بررسی و آنالیز تک تک فریم‌های نمایش داده شده در یک ثانیه، نرخ فریم حقیقی آن به دست می‌آید. لازم به ذکر است چون دستکاری نرخ فریم به صورت نرم‌افزاری صورت می‌گیرد، در نتیجه ابزارهایی چون FFmpeg و VLC که از طریق متادیتای استریم نرخ فریم را نمایش می‌دهند نیز به اشتباه اعلام می‌کنند.



تصویر ۹: نرخ فریم حقیقی دوربین



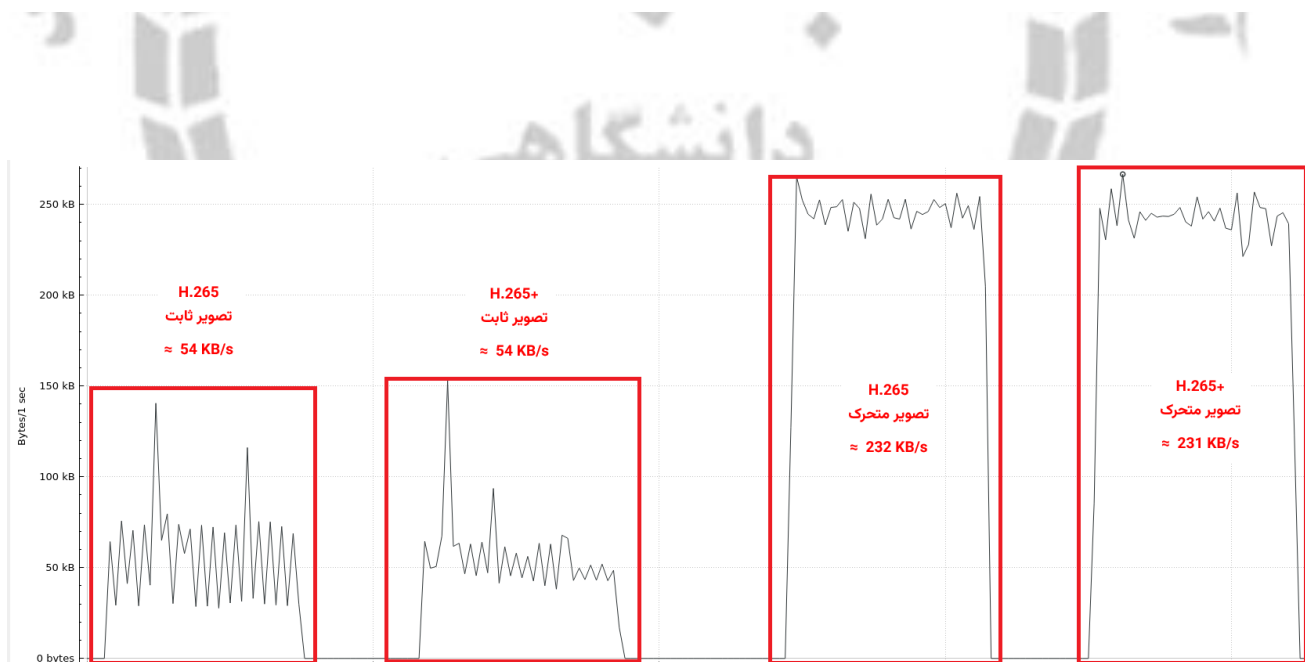
تصویر ۱۰: نرخ فریم نادرست نمایش داده شده در VLC

آزمون اندازه‌گیری نرخ بیت (Bitrate) دوربین:

مطابق این آزمون عملکرد کدک‌های پیاده‌سازی شده در دوربین را در تصویر برداری ثابت و متحرک اندازه‌گیری می‌کنیم. طبق این آزمون صحت پیاده‌سازی کدک‌ها و میزان اشغال پهنای باند شبکه توسط دوربین بررسی می‌شود.



تصویر ۱۱: نمودار و میانگین نرخ بیت برای کدک H.264



تصویر ۱۲: نمودار و میانگین نرخ بیت برای کدک H.265

آزمون‌های تست نفوذ دوربین:

۱. اسکن پورت‌های باز دوربین

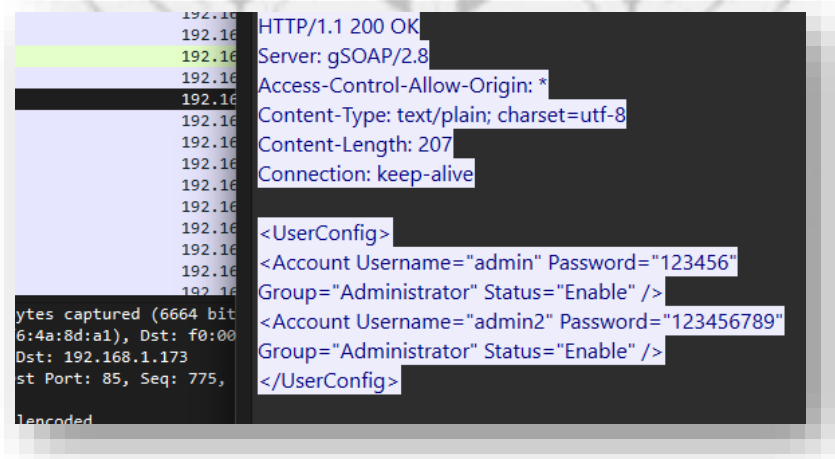
باز بودن پورت‌های غیرضروری در دوربین‌های مداربسته می‌تواند مشکلات امنیتی جدی ایجاد کند. در واقع، هر پورت باز، یک نقطه ورودی بالقوه برای نفوذگران است. اگر پورت‌های مدیریتی یا پورت‌هایی که برای انتقال تصویر استفاده می‌شوند (مانند پورت ۸۰ برای HTTP، پورت ۵۵۴ برای RTSP و غیره) بدون تدابیر امنیتی مناسب باز باشند، هکرها می‌توانند به راحتی به دوربین دسترسی پیدا کنند، تصاویر را مشاهده کنند، تنظیمات را تغییر دهند یا حتی کنترل دوربین را به دست بگیرند.

۲. بهره‌گیری از پروتکل TLS

TLS یک پروتکل رمزنگاری است که ارتباطات بین دو نقطه (مثلاً دوربین و مرورگر یا نرم‌افزار مدیریت تصاویر) را ایمن می‌کند. این پروتکل تضمین می‌کند که داده‌های ارسالی بین این دو نقطه، رمزگذاری شده و از شنود، تغییر یا دسترسی غیرمجاز محافظت می‌شوند؛ بدون TLS، هر کسی که به شبکه دسترسی داشته باشد، می‌تواند ترافیک ارسالی از دوربین را شنود کند و تصاویر، صداها و حتی رمزهای عبور را به دست آورد. مثلاً در حمله Man-in-the-Middle (MITM)، مهاجم می‌تواند بین دوربین و کاربر قرار بگیرد و ترافیک را دستکاری کند، تصاویر را تغییر دهد یا حتی اطلاعات جعلی ارسال کند.

۳. بهره‌گیری از Basic/Digest Authentication

این روش‌ها برای احراز هویت کاربرانی که می‌خواهند به دوربین دسترسی پیدا کنند، استفاده می‌شوند. Basic Authentication اطلاعات کاربری (نام کاربری و رمز عبور) را به صورت رمزگذاری نشده (Base64) ارسال می‌کند که به راحتی قابل رمزگشایی است. Digest Authentication یک روش امن‌تر است که از هش کردن رمز عبور برای احراز هویت استفاده می‌کند و از ارسال مستقیم رمز عبور جلوگیری می‌کند.



تصویر ۱۳: نمونه یک دوربین تولید داخل بدون بهره‌گیری از Authentication

```

POST /tdkcg HTTP/1.1
Host: 192.168.226.202
Connection: keep-alive
Content-Length: 289
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 Edg/131.0.0.0
Accept: application/xml, text/xml, */*; q=0.01
Content-Type: application/xml
Origin: http://192.168.226.202
Referer: http://192.168.226.202/index.html
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

<?xml version="1.0" encoding="utf-8"?><envelope><header><security>usernetoken</security><username>admin</username><password>tMtdM6eLsnGgbMF2UmJULw==</password><nc>Pdlddb5jGSX4HiThp2ohJvsRKez313m</nc></header><body><command>get.network.b
ase</command><content></content></body></envelope>

```

تصویر ۱۴: نمونه یک دوربین تولید داخل با بهره‌گیری از Authentication

۴. بدست آوردن لیست مسیرهای RTSP پنهان دوربین با روش Brute Force

دوربین‌های مدار بسته به جهت افزایش امنیت امکان تغییر مسیر RTSP را در Firmware دوربین برای کاربر فراهم می‌کنند. اما مشاهده شده است در بسیاری از دوربین‌ها از مسیرهای RTSP متعددی امکان گرفتن استریم فراهم است.

صورت کلی یک لینک RTSP به فرم زیر است:

rtsp://username:password@ip_address:port/path

```

x
192.168.1.32
554
basic
admin
123456

//
/stream0
/stream1
/0/video1
/1/h264major
/1/stream1
/CH001.sdp
/MediaInput/h264
/MediaInput/mpeg4
/Streaming/Channels/1
/Streaming/Unicast/channels/101
/StreamingSetting?version=1.0&action=getRTSPStream&ChannelID=1&ChannelName=Channel1
/VideoInput/1/h264/1
/VideoInput/1/mpeg4/1
/cam/realmonitor?channel=0&subtype=0
/cam/realmonitor?channel=1&subtype=0
/cam/realmonitor?channel=1&subtype=1
/cam/realmonitor?channel=1&subtype=1&unicast=true&proto=Onvif
/cam1/h264
/cam1/h264/multicast
/cam1/mpeg4
/cam1/mpeg4?user='username'&pwd='password'
/ch001.sdp
/ch01.264
/ch01.264?
/ch01.264?ptype=tcp

btwolame --enable-libvidstab
--enable-libx265 --enable-li
bzmq --enable-libzvbi --enabl
--enable-opengl --enable-sdl2
bmfxf --enable-libdc1394 --ena
t --enable-frei0r --enable-li
libavutil 56. 70.100 /
libavcodec 58.134.100 /
libavformat 58. 76.100 /
libavdevice 58. 13.100 /
libavfilter 7.110.100 /
libswscale 5. 9.100 /

```

تصویر ۱۵: لیست مسیرهای RTSP پنهان در یک دوربین تولید داخل

۵. انجام حملات DoS بر روی دوربین مدار بسته و بدست آوردن مقاومت دوربین در برابر این نوع حملات

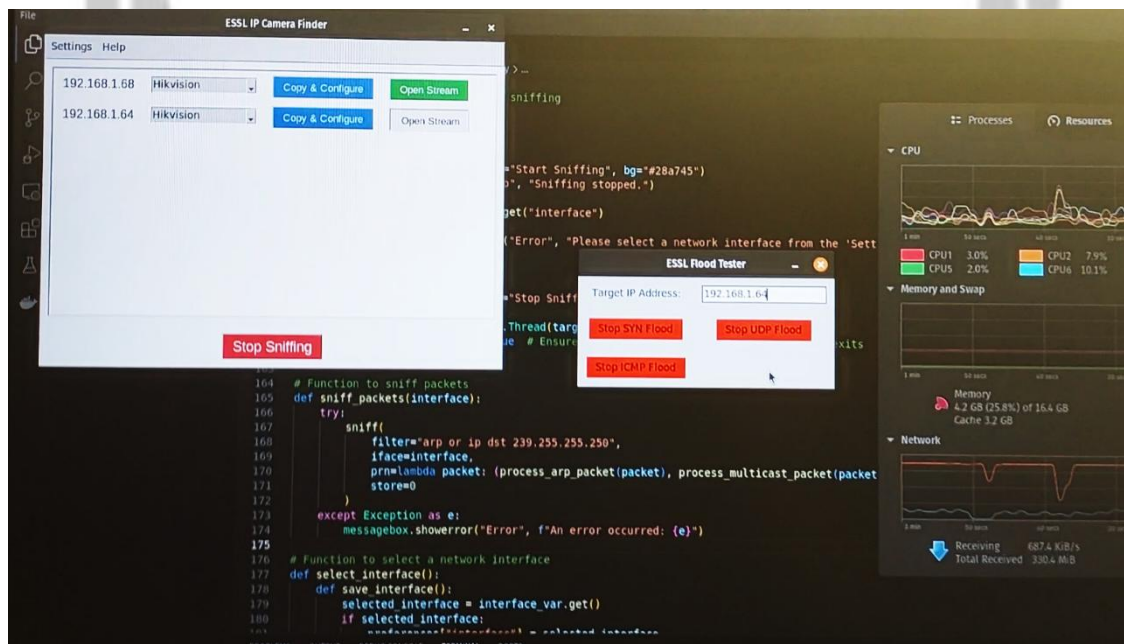
حملات (Denial of Service) DoS یا منع سرویس تلاشی برای از دسترس خارج کردن یک منبع، مانند دوربین مدار بسته است. این حملات می‌توانند به طور خاص برای دوربین‌های مدار بسته بسیار مخرب باشند، زیرا می‌توانند ضبط تصاویر، انتقال آنها و حتی دسترسی به تنظیمات دوربین را مختل کنند. در اینجا به نحوه تأثیر این حملات بر دوربین‌های مدار بسته و نکات مرتبط با آنها می‌پردازیم:

قطع ضبط و انتقال تصاویر: حملات DoS می‌توانند با اشغال پهنای باند شبکه یا منابع پردازشی دوربین، از ضبط و انتقال تصاویر جلوگیری کنند. در نتیجه، در زمان وقوع حمله، هیچ تصویری ضبط یا منتقل نخواهد شد.

اختلال در دسترسی به رابط وب دوربین: این حملات می‌توانند دسترسی به رابط وب دوربین را مختل کنند و از تغییر تنظیمات، مشاهده تصاویر زنده یا انجام سایر عملیات مدیریتی جلوگیری کنند.

ری‌استارت مکرر دوربین: در برخی موارد، حملات سنگین DoS می‌توانند باعث ری‌استارت مکرر دوربین شوند و عملکرد آن را به طور کامل مختل کنند.

آسیب‌پذیری در برابر سایر حملات: حملات DoS می‌توانند به عنوان پوششی برای سایر حملات پیچیده‌تر مورد استفاده قرار گیرند. به عنوان مثال، مهاجم می‌تواند با انجام یک حمله DoS، توجه مدیران شبکه را به خود جلب کند و در این حین، از طریق یک آسیب‌پذیری دیگر به سیستم نفوذ کند.



تصویر ۱۶: تصویری از انجام حملات DoS به دوربین مدار بسته

انواع حملات DoS بر روی دوربین‌های مداربسته:

SYN Flood: این حمله می‌تواند به طور خاص برای دوربین‌هایی که از پروتکل TCP برای ارتباط استفاده می‌کنند) مانند دسترسی به رابط وب یا انتقال تصاویر از طریق RTSP با (TCP مخرب باشد. با پر کردن حافظه دوربین با درخواست‌های SYN جعلی، دوربین قادر به پاسخگویی به درخواست‌های واقعی نخواهد بود.

UDP Flood: از آنجایی که بسیاری از دوربین‌ها از پروتکل UDP برای انتقال تصاویر استفاده می‌کنند، حملات UDP Flood می‌توانند به طور مستقیم بر جریان ویدیو تأثیر بگذارند و باعث قطع یا تأخیر در انتقال تصاویر شوند.

HTTP Flood: این نوع حمله به طور خاص رابط وب دوربین را هدف قرار می‌دهد. با ارسال تعداد زیادی درخواست HTTP به سرور وب دوربین، منابع آن اشغال شده و از پاسخگویی به درخواست‌های کاربران واقعی باز می‌ماند.

ICMP Flood و ...

۶. علاوه بر آزمون‌های معرفی شده، مواردی همچون Packet Loss، Latency، استریم، پشتیبانی از انواع پروتکل‌های شبکه، اعتبار MAC Address، امکان Multicast and ICMP Turnoff و ... مورد بررسی قرار می‌گیرند.

لازم به ذکر است برای انجام آزمون‌ها نرم افزاری در آزمایشگاه طراحی و توسعه داده شده است.