

Side-channel attacks

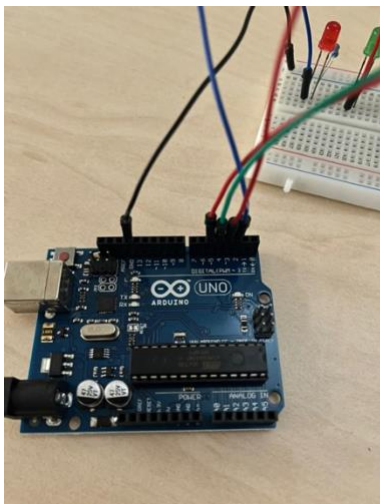
V kryptografii sú *side-channel attacks* útoky, ktoré sa snažia zneužiť informácie, ktoré priamo unikajú z fyzickej implementácie systému, na rozdiel od kryptoanalýzy, ktorá sa snaží nájsť slabiny v matematickej štruktúre algoritmu.

V tomto projekte som sa zaoberal *elektromagnetickými útokmi (EMA)*. Komponenty systému pri zmene prúdu generujú striedavé magnetické pole, ktoré ak je dostatočne silné, môže byť detegované a následne analyzované. Tieto útoky sú zvyčajne neinvazívne, teda môžeme ich uskutočniť pomocou pozorovania daného zariadenia. Zariadenia, ktoré nie sú zabezpečené voči takýmto útokom, môžu byť náchylné na zneužitie citlivých informácií.

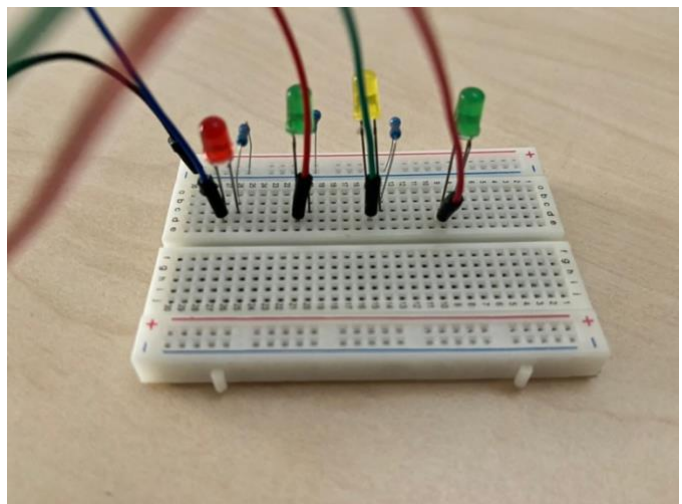
Report – zimný semester

Počas zimného semestra som sa zoznamoval s mikrokontrolérom *Arduino UNO R3* na účely odmerania jeho elektromagnetického vyžarovania pri vykonávaní aritmetických operácií. Cieľom bolo zistiť, či vieme nájsť medzi operáciami a vyžarovaním koreláciu, ktorú by sme vedeli neskôr využiť.

Vytvoril som jednoduché programy, v ktorých sa striedali aritmetické operácie $+$, $-$, $*$, $/$ a pri vykonaní danej operácie sa rozsvietilo jej príslušné LED svetielko, aby sme pri meraní vedeli rozpoznať, ktorá operácia bola vykonaná.



Obrázok 1 - Arduino UNO R3



Obrázok 2 - Breadboard so zapojenými LED svetielkami

Pri meraní sme so školiteľom použili osciloskop *Tektronix MDO4104C*. Jednu testovaciu sondu sme napojili na kryštál Arduina, ktorý sa nachádza vedľa jeho čipu a druhú sondu na anódu daného LED svetielka, aby sme vedeli, kedy bola operácia vykonaná. Výsledky tohto merania neboli presvedčivé, nakoľko nebola viditeľná korelácia medzi jednotlivými operáciami a zmenami napätia mikrokontroléru.

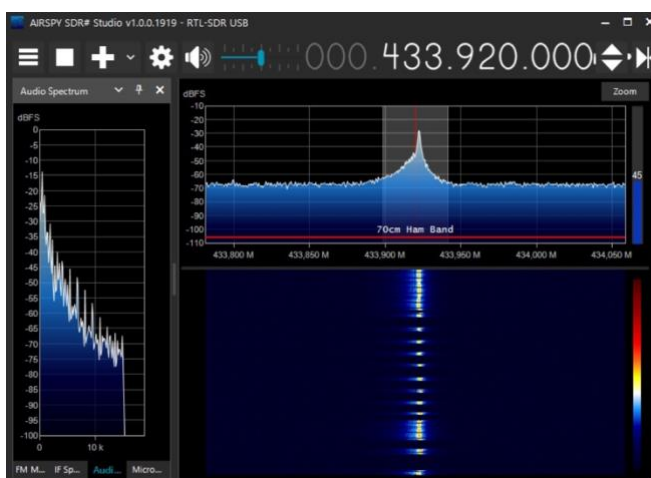
Následne sme sa snažili odmerať rádiové frekvencie (RF) kryštálu pri daných operáciách pomocou *near-field* sondy, no výsledky boli rovnaké ako pri predošlom meraní.

Po neúspešných meraniach som sa začal venovať odpočúvaniu obrazoviek pomocou *softvérovo definovaných rádií (SDR)*. Cieľom bolo vyčítať, čo je na obrazovke zariadenia bez toho, aby sme na danú obrazovku priamo videli. Pomocou SDR vieme zachytiť elektromagnetický signál, ktorý je posielaný káblom od zariadenia do obrazovky.

Zoznamoval som sa s *RTL-SDR*, ktoré sa radí medzi lacné SDR. Pri učení, ako sa s SDR pracuje som využíval aplikáciu *SDR#*.

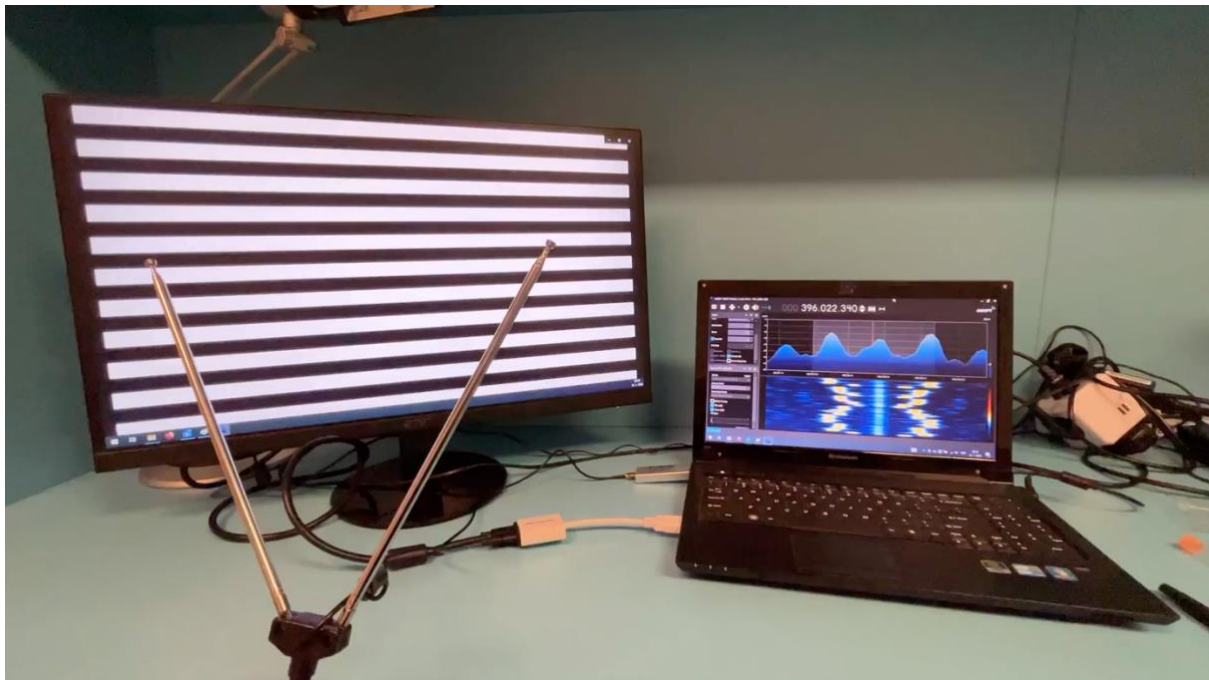


Obrázok 3 - RTL-SDR kit



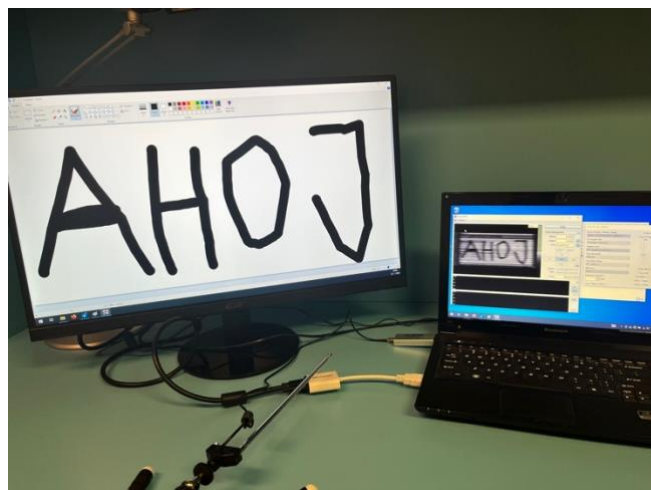
Obrázok 4 - Posielanie signálov pomocou tlačítka s frekvenciou 433,920 MHz

Následne som na monitore, ktorý bol napojený k PC pomocou redukcie z HDMI na VGA a VGA káblu, začal zobrazovať čierno-biele pásiky, pomocou ktorých som dokázal nájsť frekvenciu, pri ktorej z káblu uniká elektromagnetické vyžarovanie. Pri nájdení správnej frekvencie začne hrať melódia z rádia ([video](#)). Našiel som, že pri mojom set-upe uniká najviac signálov pri frekvencii ~396 MHz.



Video 1 - Zachytenie unikajúceho signálu z káblu

Po nájdení správnej frekvencie som využil software toolkit [TempestSDR](#), ktorý dokáže z nájdených elektromagnetických vĺn vyhotoviť čierno-biely obraz v reálnom čase pomocou mapovania sily elektromagnetickej vlny k jej príslušnému odtieňu čiernej.



Obrázok 5 - Využitie TempestSDR k vyhotoveniu obrazu

Pri meraní som narazil na viacero skutočností. Prvé merania som vykonával bez redukcie z HDMI na VGA. Elektromagnetické vlny boli pri týchto meraniach veľmi slabé – môj VGA kábel je pravdepodobne ošetrovaný voči úniku elektromagnetických vln. Pochopiteľne, aj vyhotovený obraz cez TempestSDR bol veľmi zlý a nepoužiteľný.

Po zapojení redukcie sa sila elektromagnetických vln drasticky zväčšila. Možno usúdiť, že pri konverzii je únik elektromagnetických vln zväčšený a pri použití redukcie sa môžeme vystaviť nebezpečenstvu pri práci s citlivými informáciami na obrazovke.

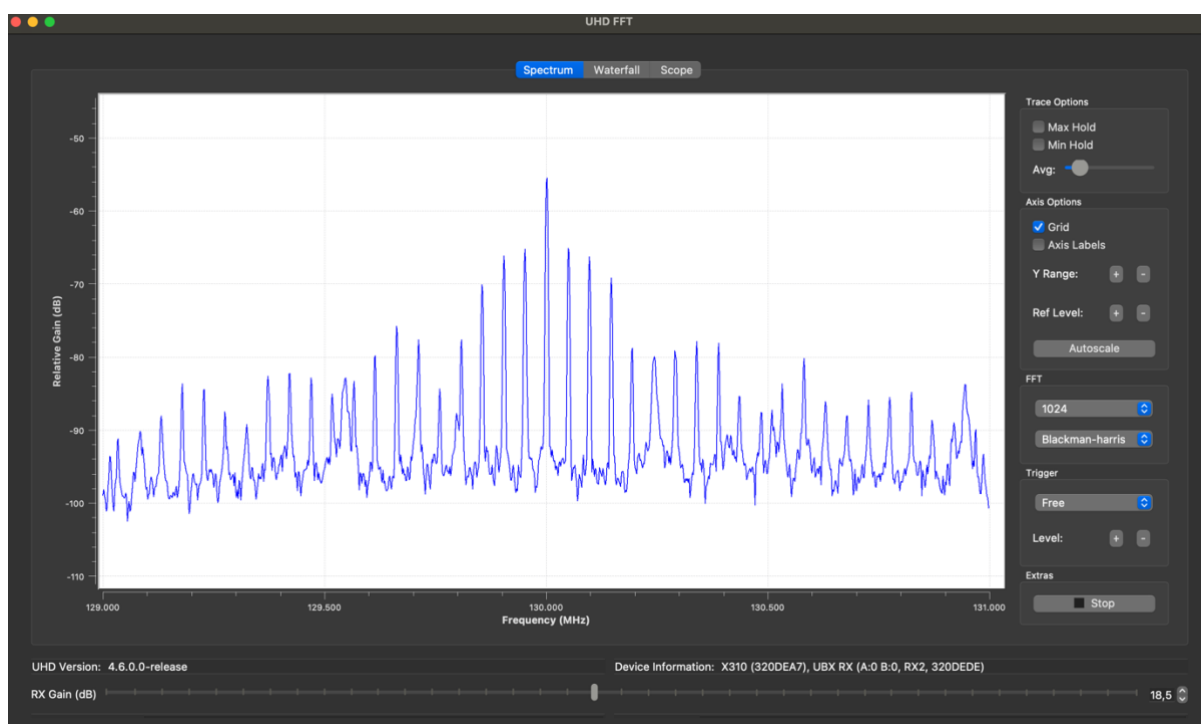
Následne som testoval, aký dobrý obraz dokážeme vyhotoviť s rastúcou vzdialenosťou medzi anténou a káblom. Obraz bol prakticky rovnaký pri vzdialenostiach do 30 cm. Pri väčších vzdialenostiach sa obraz pochopiteľne zhoršoval až kým úplne nezanikol.

Report – letný semester

Počas letného semestra som sa zoznamoval s inými SDR, najmä s *USRP X310*, no taktiež s *HackRF One* na účely odpočúvania obrazu s *TempestSDR*. Cieľom bolo zistiť, ako vyhotoviť čo najlepší obraz, porovnať zachytený obraz medzi SDR z iných cenových kategórií, no taktiež nájsť možné nedostatky, či limitácie *TempestSDR*.

Príprava

Na začiatku semestra som sa učil pracovať s *USRP X310*. Pre tieto účely som vyskúšal programy *uhd_fft* a *inspectrum*, pomocou ktorých vieme vizualizovať spektrum na danej frekvencii, resp. analyzovať zachytené signály z *USRP*. Pomocou *uhd_fft* a osciloskopu *Tektronix MDO4104C* sme našli frekvenciu, pri ktorej zachytený signál bol najsilnejší (~130 MHz).



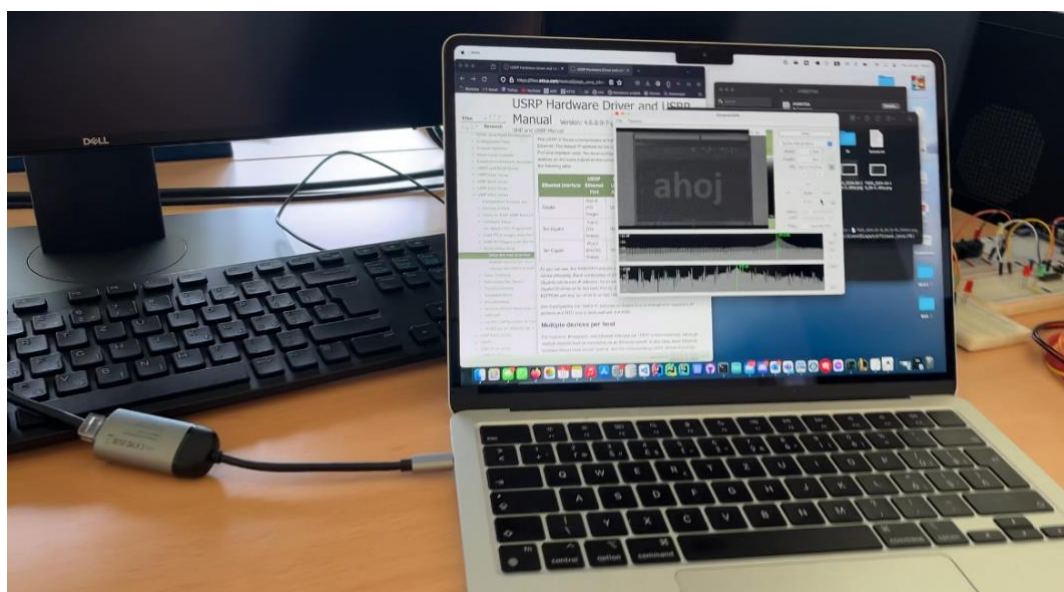
Obrázok 6 - *uhd_fft* pri frekv. 130 MHz

Predtým, ako sme mohli použiť *TempestSDR* s *USRP*, bolo potrebné aplikáciu spojzduť. Keďže toolkit *TempestSDR* bol vytvorený v roku 2014, obsahoval nedostatky, kvôli ktorým sa nedal skompilovať. Jeho *Makefile*

obsahoval nekorektné cesty na linkovanie knižníc *uhd* a *boost*, ak používateľ mal systém s macOS alebo Linux. Postup, ako tento problém opraviť, som opísal [tu](#).

Útok na monitor

Útok prebiehal tak, že som otvoril obrázok na monitore cieľového zariadenia. Monitor mal rozlíšenie *1024x768 pixelov* a bežal pri obnovovacej frekvencii *59,94 Hz*. K cieľovému počítaču bol napojený pomocou *HDMI-VGA redukcie*. Anténu SDR som priblížil k spomínanej redukcii a na útočníkovom počítači som spustil *TempestSDR* pri frekvencii 130 MHz. [Video](#).



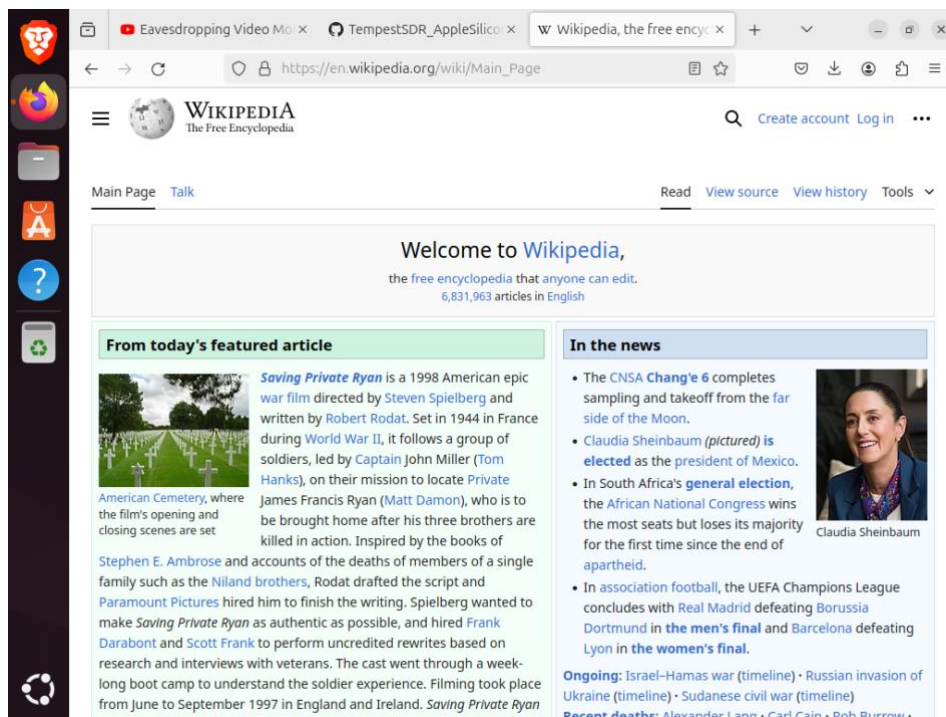
Obrázok 7 - Útočník, TempestSDR + SDR



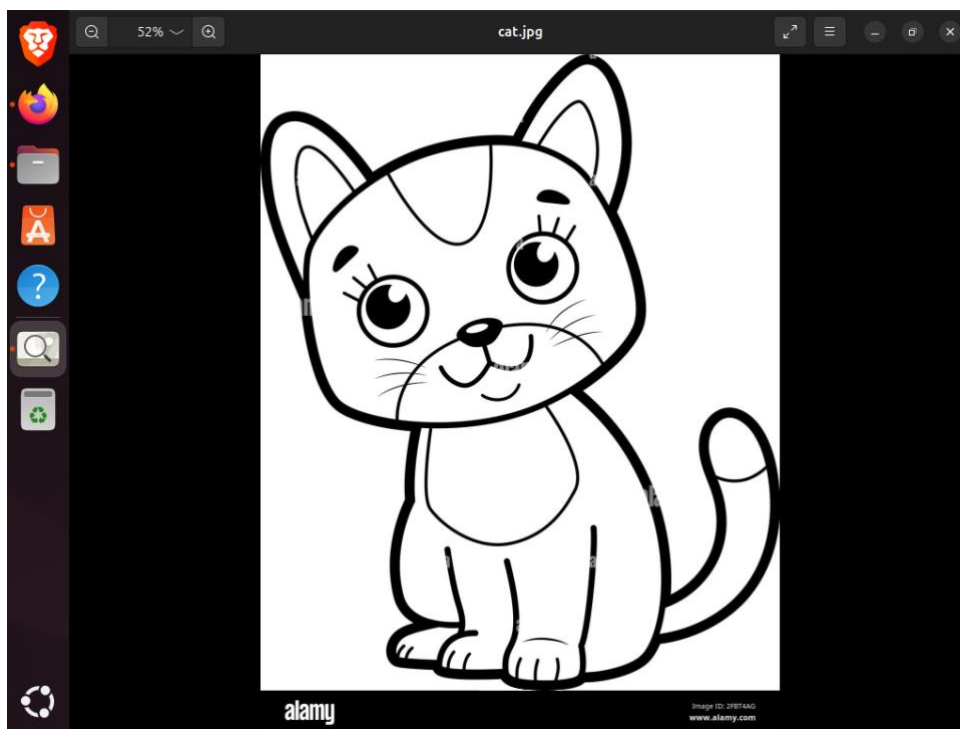
Obrázok 8 - Cieľ, Monitor + Redukcia

Porovnanie

Po spojazdnení potrebného softvéru som začal odpočúvať obraz s dostupnými SDR na účely porovnania. Ako referenčné obrázky som využil *Obrázok 9* a *Obrázok 10*.

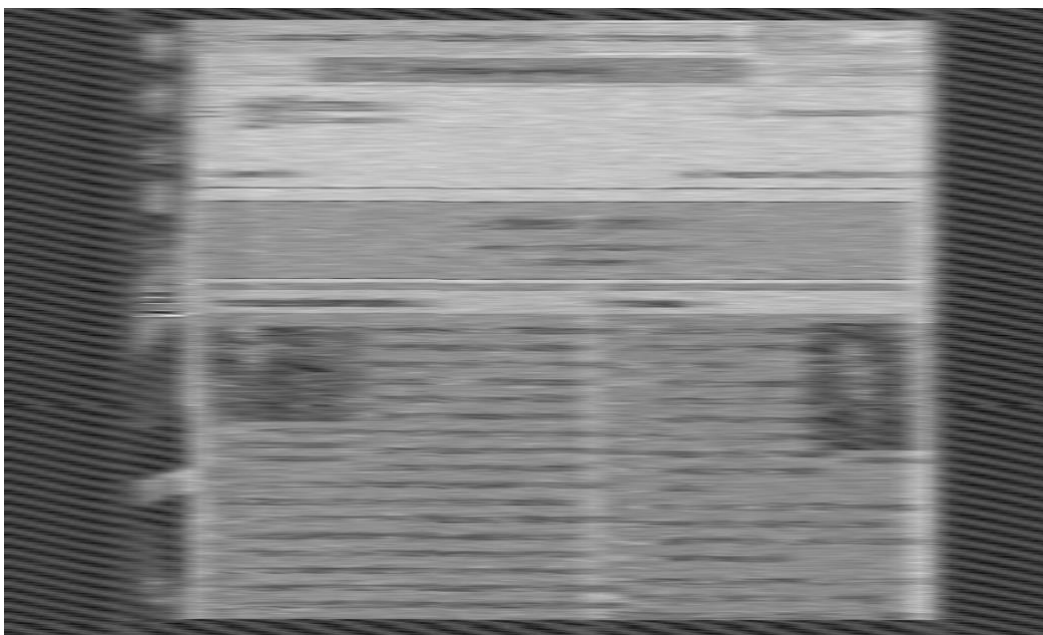


Obrázok 9 – Úvodná stránka Wikipédie



Obrázok 10 – Mačka

Obraz vyhotovený pomocou low-end SDR, *RTL-SDR*:



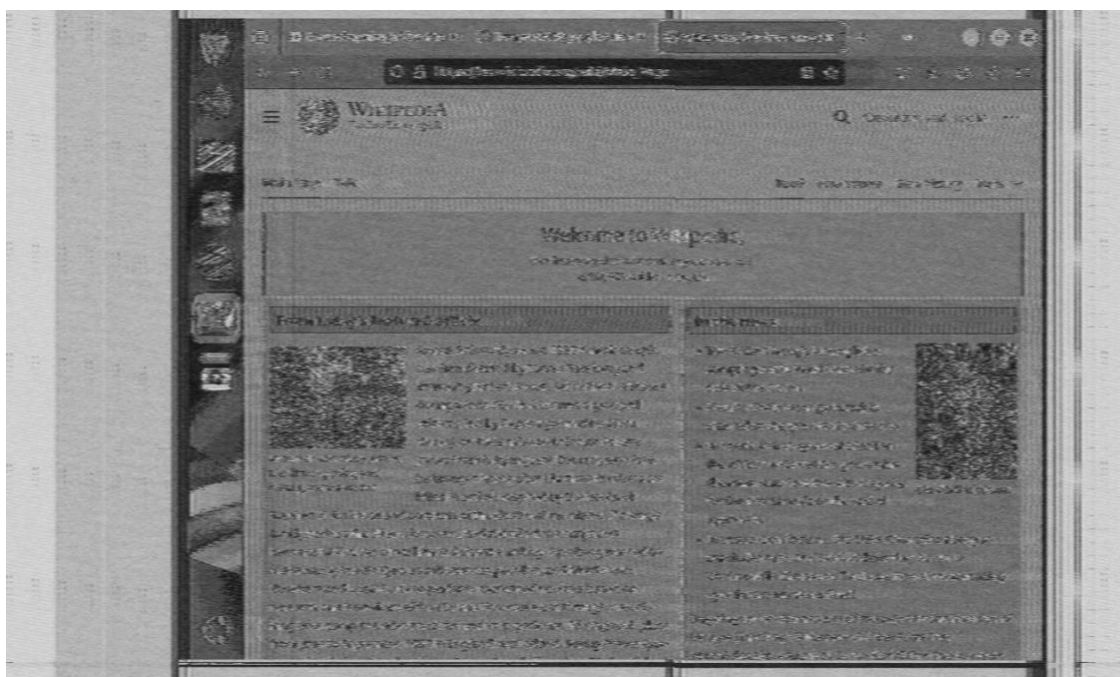
Obrázok 11 - RTL-SDR, Wikipedia



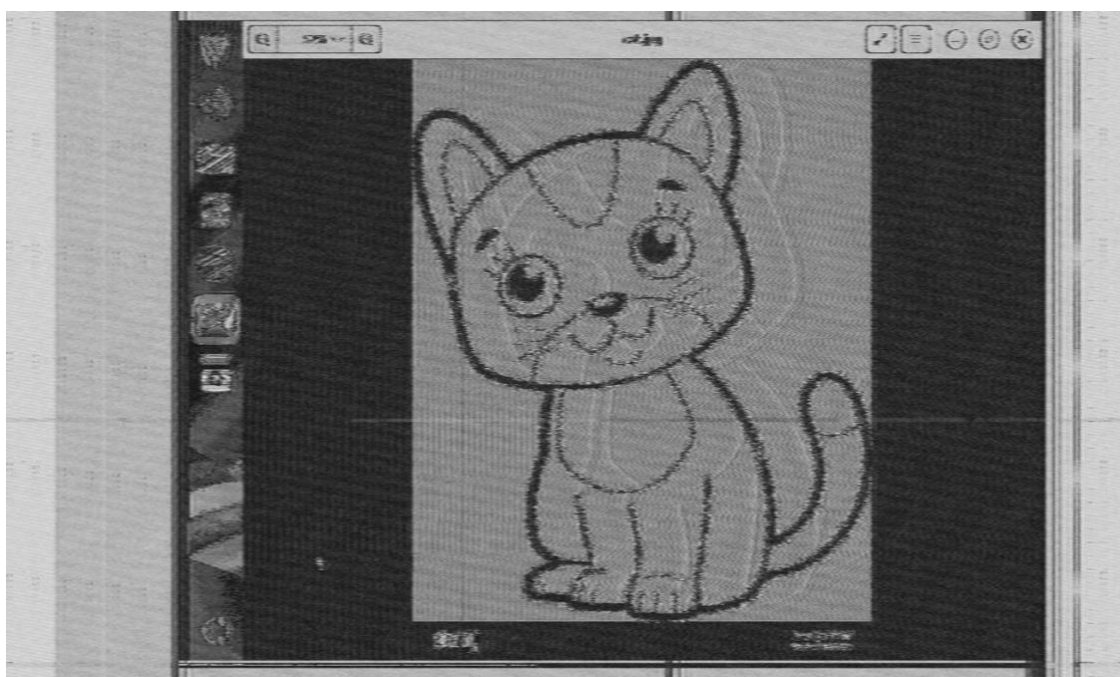
Obrázok 12 - RTL-SDR, Mačka

Ako môžeme vidieť, zachytený obraz pomocou *RTL-SDR* je neuspokojivý. Navyše, jeho nízky sample rate ($2,56\text{ MS/s}$) znamenal, že ak by sme nevedeli presnú špecifikáciu cieľového monitora, hľadanie požadovanej frekvencie by bolo veľmi prácne. Môžeme usúdiť, že na reálny útok by toto SDR nebolo vhodné.

Obraz vyhotovený pomocou medium-end SDR, *HackRF One*:



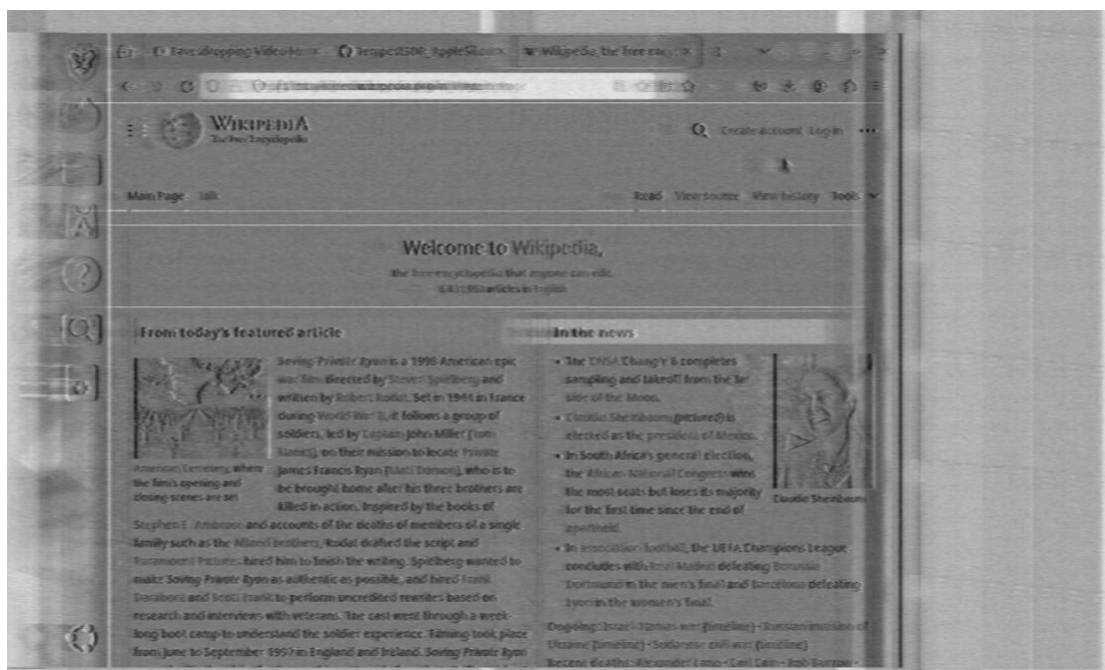
Obrázok 13 - *HackRF One*, Wikipedia



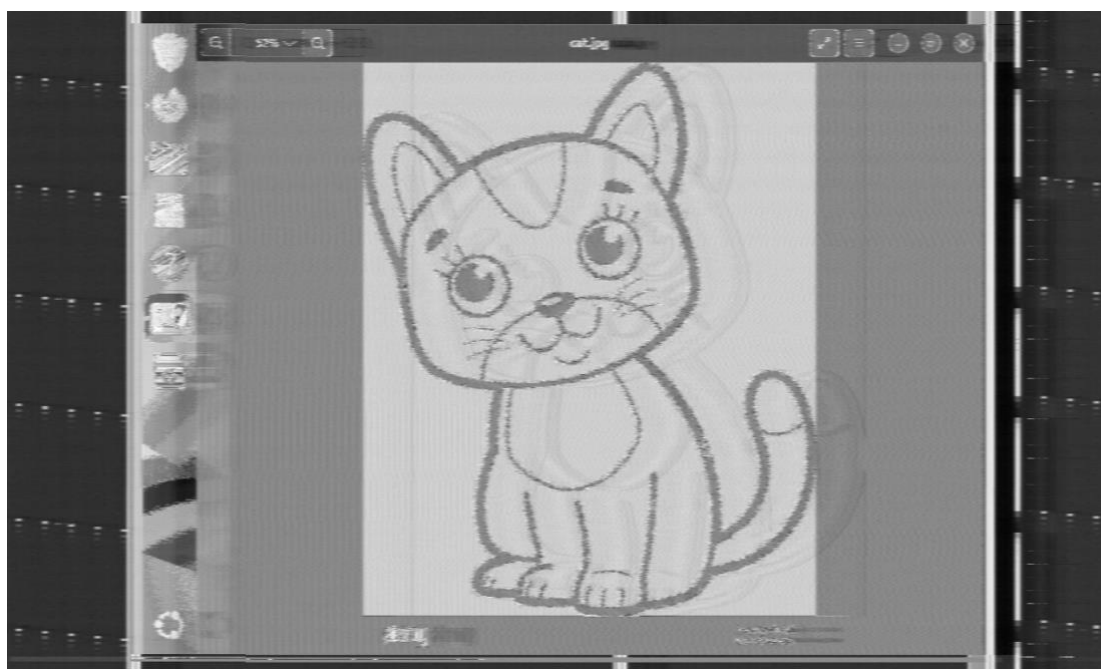
Obrázok 14 - *HackRF One*, Mačka

Použitie *HackRF One* priviedlo značné zlepšenie. Z obrazu je možné jasne dedukovať, čo náš cieľ na počítači robí. Jeho sample rate (20 MS/s) nám taktiež umožnil rýchlejšie nájdenie správnej frekvencie, čo drasticky znižuje potrebný čas na prípravu. Nedostatkom je, že menší text nie je čitateľný.

Obraz vyhotovený pomocou high-end SDR, *USRP X310*:



Obrázok 15 - *USRP X310*, Wikipedia

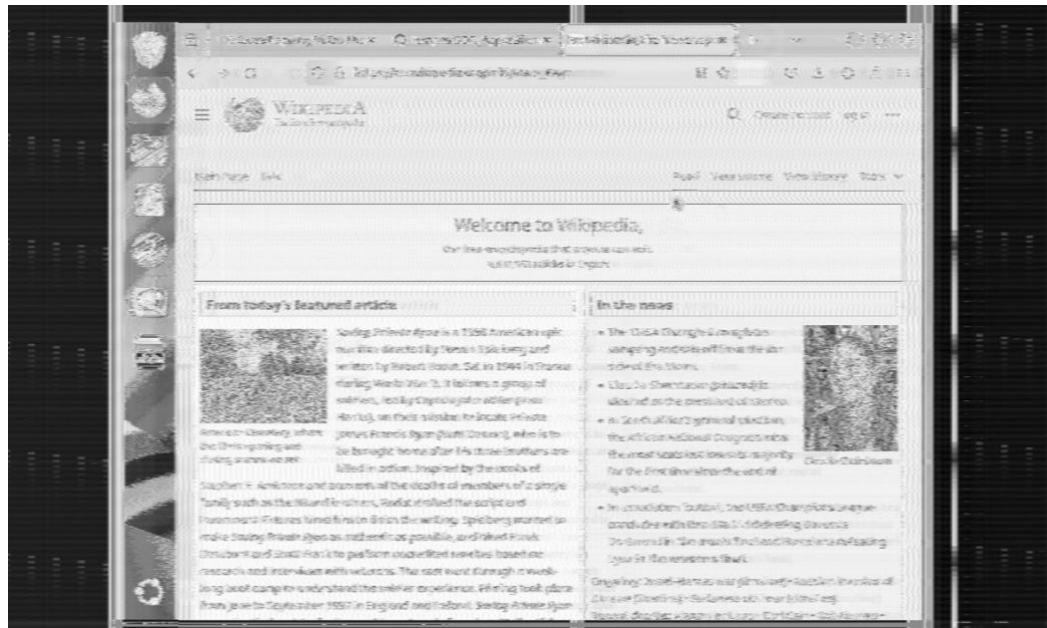


Obrázok 16 - *USRP X310*, Mačka

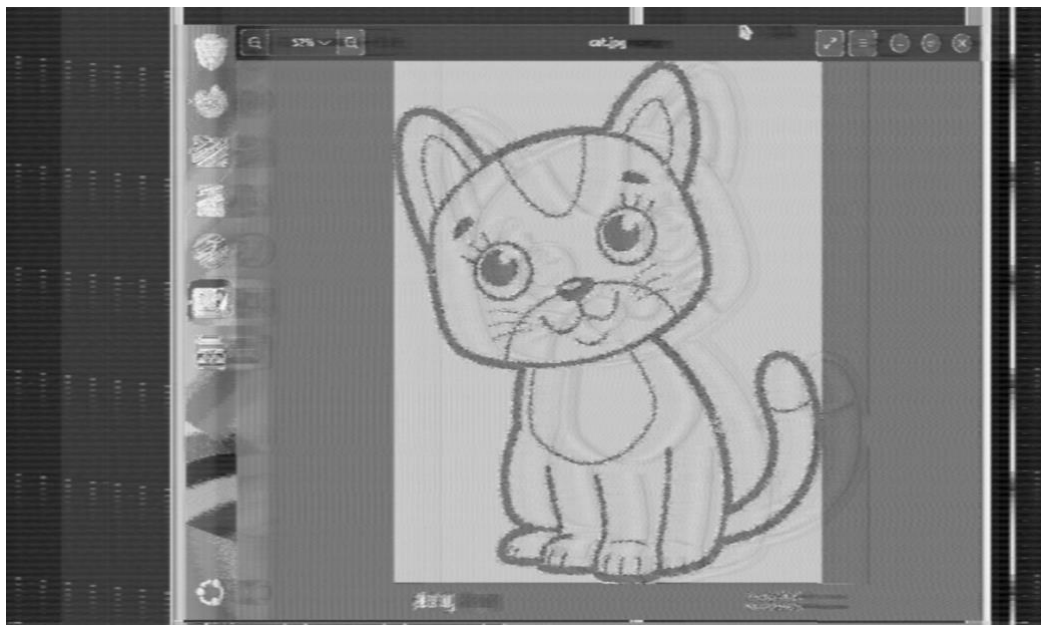
USRP X310 je ideálny kandidát na útok. Má vysoký bandwidth (160 MHz). Nie je až tak obmedzený na diaľku – útok je možný vykonať aj z väčšej vzdialenosti, no potrebujeme na to použiť správnu anténu. Text je čitateľný.

Avšak, keďže *USRP* je mohutnejšie ako predošlé SDR, útočník má v porovnaní s predošlými SDR menšiu mobilitu.

Obraz vyhotovený pomocou high-end SDR, *USRP X310* a zosilňovača *TQP3M9037-LNA*:



Obrázok 17 - *USRP X310* + AMP, Wikipedia



Obrázok 18 - *USRP X310* + AMP, Mačka

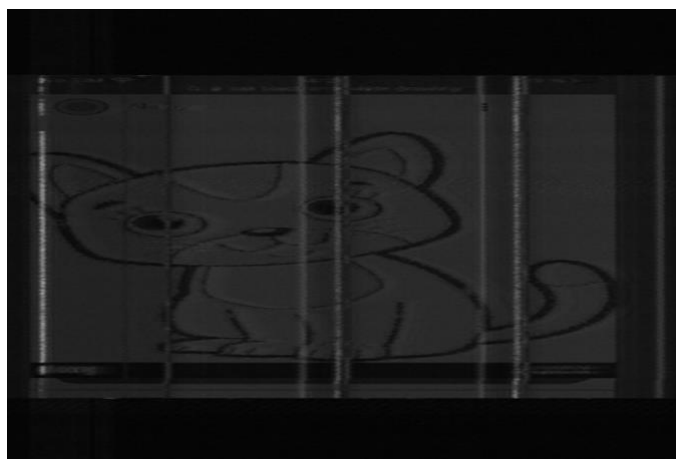
Použitie zosilňovača má svoje benefity, no aj nedostatky. Zosilňovač nám zosilnil aj nechcené frekvencie, kvôli ktorým môžeme na obraze vidieť šum a menší text sa číta ťažšie. Naopak, vzdialenosť, z ktorej môžeme vykonávať útok je väčšia. Môžeme usúdiť, že pred použitím zosilňovača by bolo vhodné použiť filter, ktorý by tieto nechcené frekvencie odfiltroval.

Útok na mobil

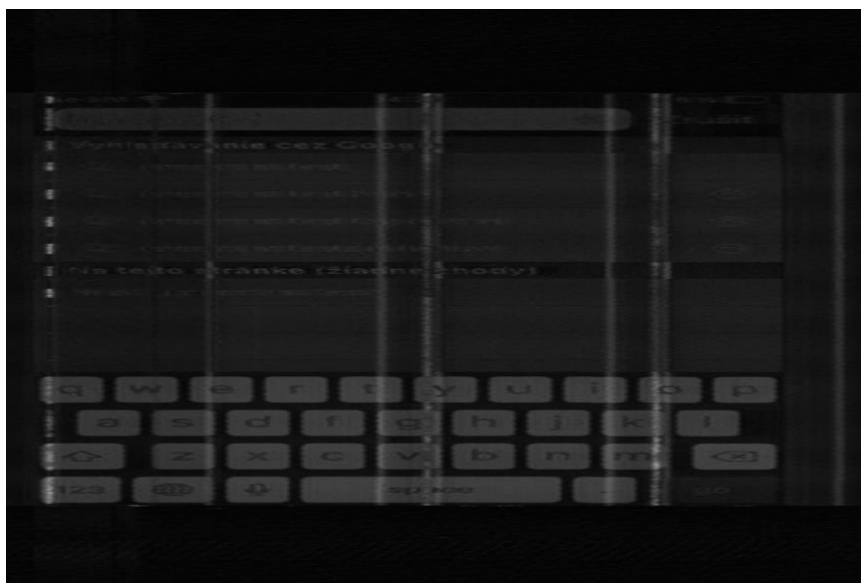
Kým doteraz som odpočúval monitory, vyskúšal som aj odpočúvanie mobilu (*Apple iPhone 6S*). Frekvencia, pri ktorej z mobilu unikalo najviac signálov, bola *293 MHz*. Na to, aby som zachytil obraz, musel som použiť zosilňovač, keďže bez neho bol obraz nepoužiteľný. Taktiež vzdialenosť, z ktorej som útok vykonával, bola veľmi malá. Použil som *USRP X310*.



Obrázok 19 - *iPhone 6S*, Útok



Obrázok 20 - *iPhone 6S*, Mačka



Obrázok 21 - iPhone 6S, Text

Odpočúvaný obraz je zreteľný. Značným nedostatkom je, že útok musíme vykonávať z veľmi malej vzdialenosti (~1 cm). Kvôli tomu môžeme skonštatovať, že v reálnom svete by bolo veľmi ťažké vykonať takýto útok.

TempestSDR a farby

Pri meraní s rôznymi SDR sme spozorovali niečo nečakané – *TempestSDR* nie je spoľahlivý pri odhadoch farieb. Prejaví sa to najmä pri obrazoch, na ktorých je viacero odtieňov rovnakej farby. *TempestSDR* ich zvykne odhadnúť ako úplne iné farby a výsledný obraz je nepresný. Tento jav môžeme vidieť na nasledujúcej ukážke:

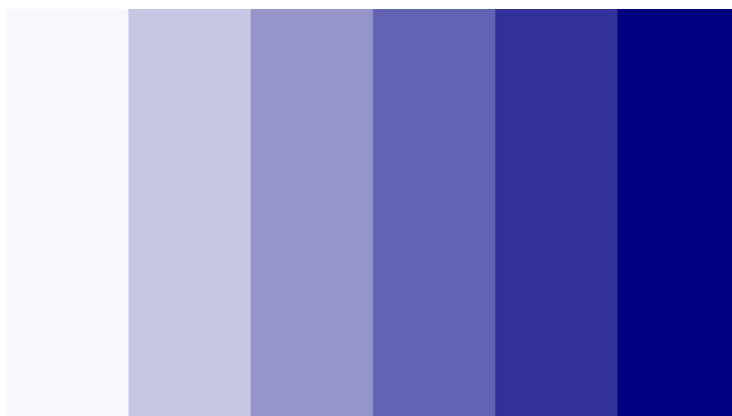


Obrázok 22 - Wikipedia, Farby

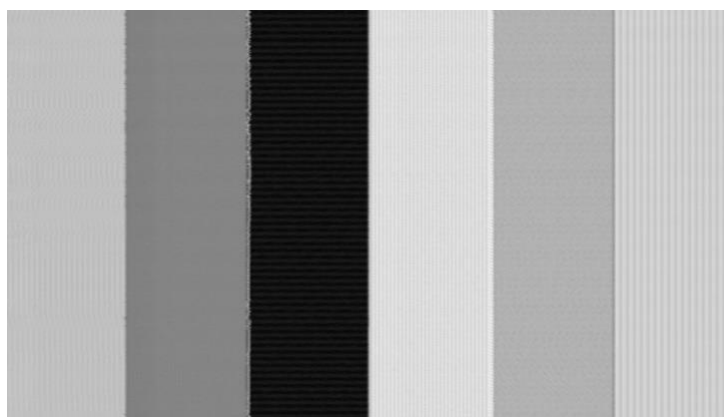


Obrázok 23 - Wikipedia, *TempestSDR* Farby

Ak sa pozrieme bližšie na *Obrázok 22*, zistíme, že okolo rámčeka v strede je tieň, ktorý voľným okom až tak nevidíme. Avšak, *TempestSDR* to interpretuje ako celkom inú farbu a prejaví sa to zvláštnym „vlnením“ okolo rámčeka na *Obrázku 23*. Tento jav môžeme spozorovať lepšie na nasledujúcich obrázkoch:



Obrázok 24 - Gradient modrej farby



Obrázok 25 - *TempestSDR*, Gradient modrej farby

Záver

Počas tohto semestra som získal cenné skúsenosti v oblasti postranných útokov. Naučil som sa základy pri práci s SDR a osciloskopom. Zistil som, na akom princípe funguje software toolkit *TempestSDR* a ako s ním vyťažiť čo najviac s dostupnými prostriedkami. Spoznal som aj jeho nedostatky a možné aplikácie v reálnom svete, z ktorých môžeme ďalej ťažiť.

Študent: Filip Tuch

Školiteľ: RNDr. Richard Ostertág PhD.