IoT device Period/Frequency (in lab)

oit-dns/find-period-active-pcaps.ipynb

Algorithm to find period of domain

1. For each domain in [domain|time] dataset for a source IP
2. Continue if the domain is queried for at least ½ the time of the total pcap - otherwise regard it as bursty [No period]
3. Continue if there are at least THRESH (=10) number of queries for that domain
4. Calculate the sampling time Ts as ½ of the minimum diff(1) between subsequent queries. However set min Ts as 1.0 second. Sampling freq fs = 1/Ts
5. Bin dns query timings using Ts (numpy.bincount(x/Ts))
6. Get periodogram freq and PSD using scipy.signal.periodogram over binned data using fs
7. Find the max PSD and its corresponding frequency value, period_freq. Period (in sec) is 1/period_freq
8. Confirm that the period is less than half the total time of pcap (or half the time of the domain queried?)

TODO: if signal is non-periodic, current algorithm sometimes still calculates period. Need better filtering than step 2, 3, and 8 to avoid this.

Datasets

	Device	Collection Time	Activity Mode	Notes/ Configuration
D01	Nest Thermostat (10.0.0.7)	45 hrs	Normal Home Use	IoT-dumps/nest/1448061849.pcap (nestthermo_homeuse_20151120_45hr.csv)
D02	Amazon Echo (10.0.0.4)	16 hrs	Background	IoT-dumps/echo/1455151444.pcap (echo_lab_20160211_16hr.csv)

D03a	Nest Dropcam (10.0.0.9)	24 hr	Background/No video	IoT_long_dumps/nestcam_sharxcam_20160702_24hr.pcap
D03b	Nest Dropcam	13 hr	Active Video	nestcam_sharxcam_motion_20160704_13hr.pcap
D03b	Nest Dropcam	2 hr	Active Video + Viewstream	nestcam_sharxcam_motion_viewstream_20160704_2hr_00001_20160704153626.pcap
D04a	Sharx Security Camera (10.0.0.8)	24 hr	Background/No video	IoT_long_dumps/nestcam_sharxcam_20160702_24hr.pcap
D04b	Sharx Security Camera	13 hr	Active Video	nestcam_sharxcam_motion_20160704_13hr.pcap
D04c	Sharx Security Camera	2 hr	Active Video + Viewstream	nestcam_sharxcam_motion_viewstream_20160704_2hr_00001_20160704153626.pcap
D05a	SmartThings (10.42.0.89)	4 hrs	Background	smartthings_alone_20160702_4hr.pcap
D05b	SmartThings + Door Sensor	14 hrs	Background	smartthings_doorsensor_20160703_14hr.pcap
D05c	SmartThings + SmartSocket	10 hrs	Background	smartthings_smartsocket_20160704_10hr.pcap
D05d	SmartThings + Door Sensor + SmartSocket	14 hrs	Background	smartthings_smartsocket_doors

				ensor_20160706_14hr.pcap

Results

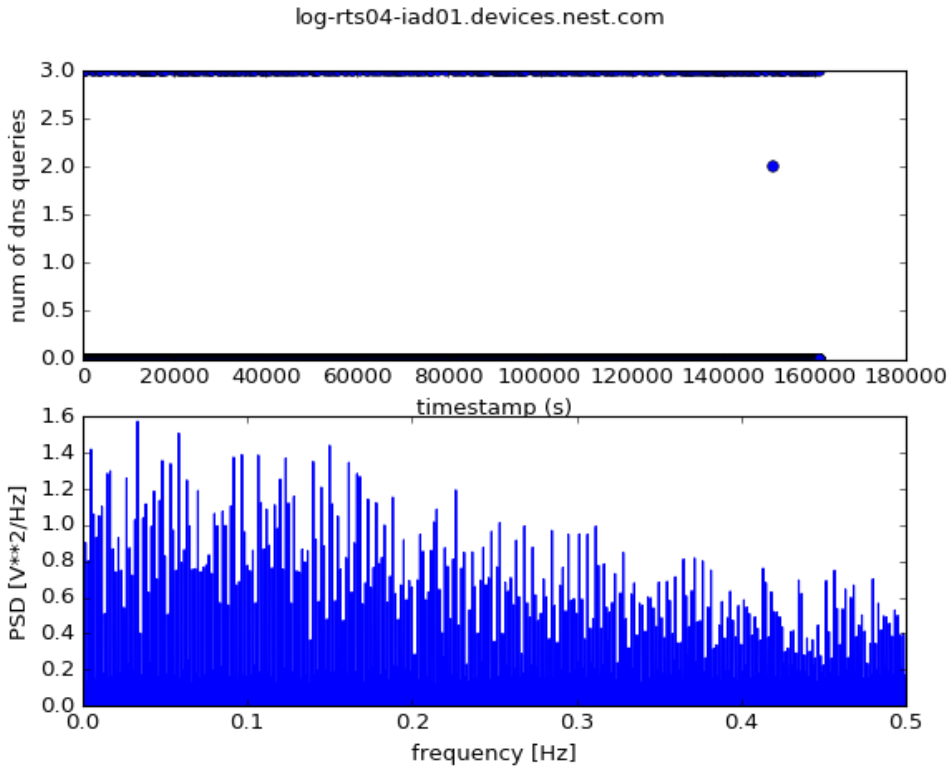
We analyzed DNS query patterns for 5 devices during background mode and continuous long term use.

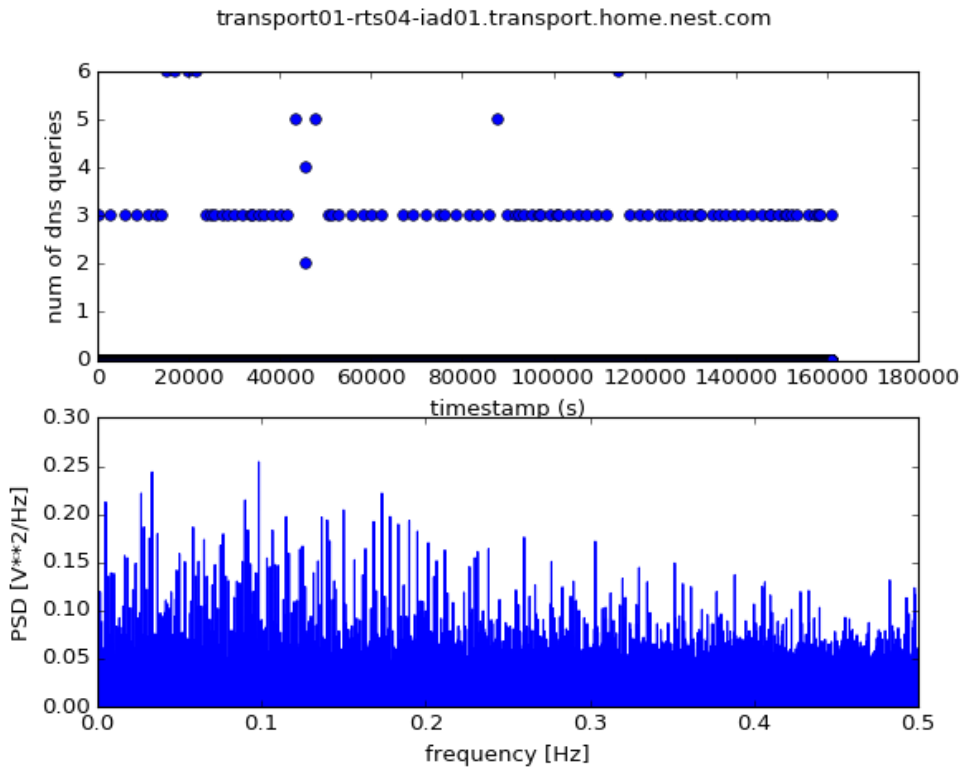
- Nest thermostat has 3 domains that are queried consistently during background mode. 2 domains have a period of 30 s and one has a period of 10 s. 2 domains are device log related while one transmits incoming weather information.
- Amazon echo periodically queries at least 2 domains with periods 300s for device related domain and ~600 sec for timing information.
- Nest dropcam periodically queries its device domain and ntp every ~47s. However, this is only during background mode. If there is motion or the dropcam is in use, no more DNS queries are performed as there is a consistent secure connection over port 443 sending data.
- Sharx IP camera consistently queries its domain and ntp every 10s in background mode. However if the camera is in use detecting motion, or someone is viewing the stream, its frequency of contacting sharxsecurity.com may change. Additionally, based on the mode and settings (ftp enabled/ email updates) it also sends information to the server as requested. This period was probably set to 5-10 sec however we see multiple peaks in our PSD plot due to aliasing.
- Smartthings device only queries DC.smartthings.com when actively being used. In background state it only performs an initial query and periodically contacts only ntp. When used alone, the ntp server is contacted every 120s. However when paired with a sensor (such as door sensor or smart socket), in background mode, smartthings queries ntp every 600s. Contact to DC.smartthings.com is bursty and sporadic. We should avoid calculating period for this domain (todo).

Nest Thermostat (D01)

Domain	Num of queries	Period_freq (Hz)	Period (s)
frontdoor.nest.com	6		
log-rts04-iad01.devices.nest.com	836	0.033326	30.01
time.nest.com	11		

transport01-rts04-iad01.transport.home.nest.com	297	0.098326	10.17
weather.nest.com	225	0.033326	30.01

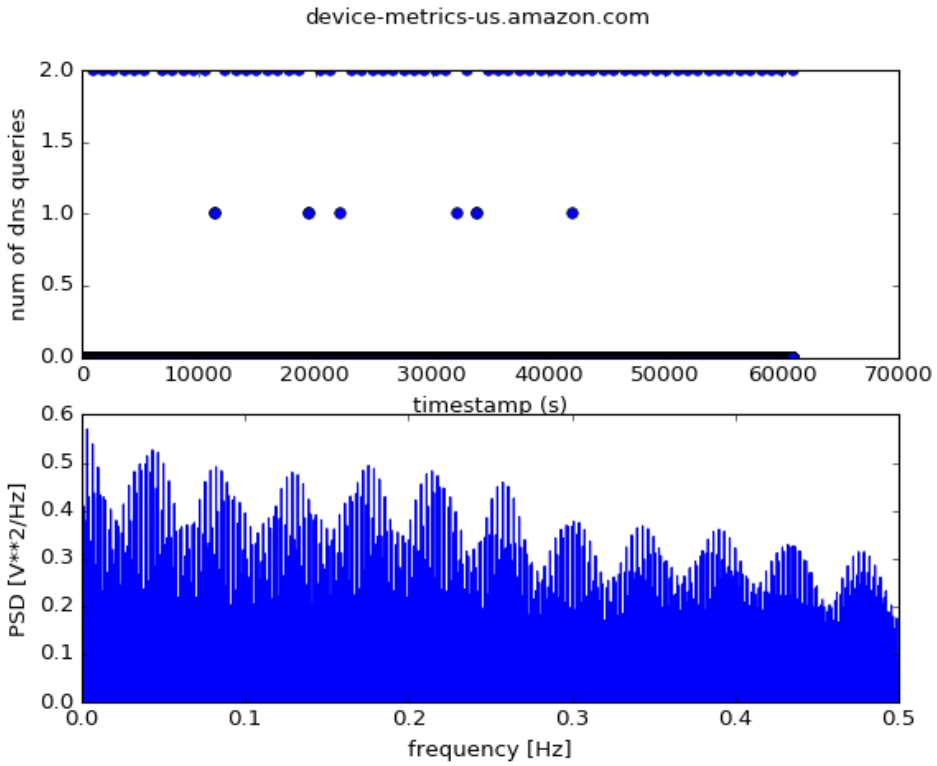


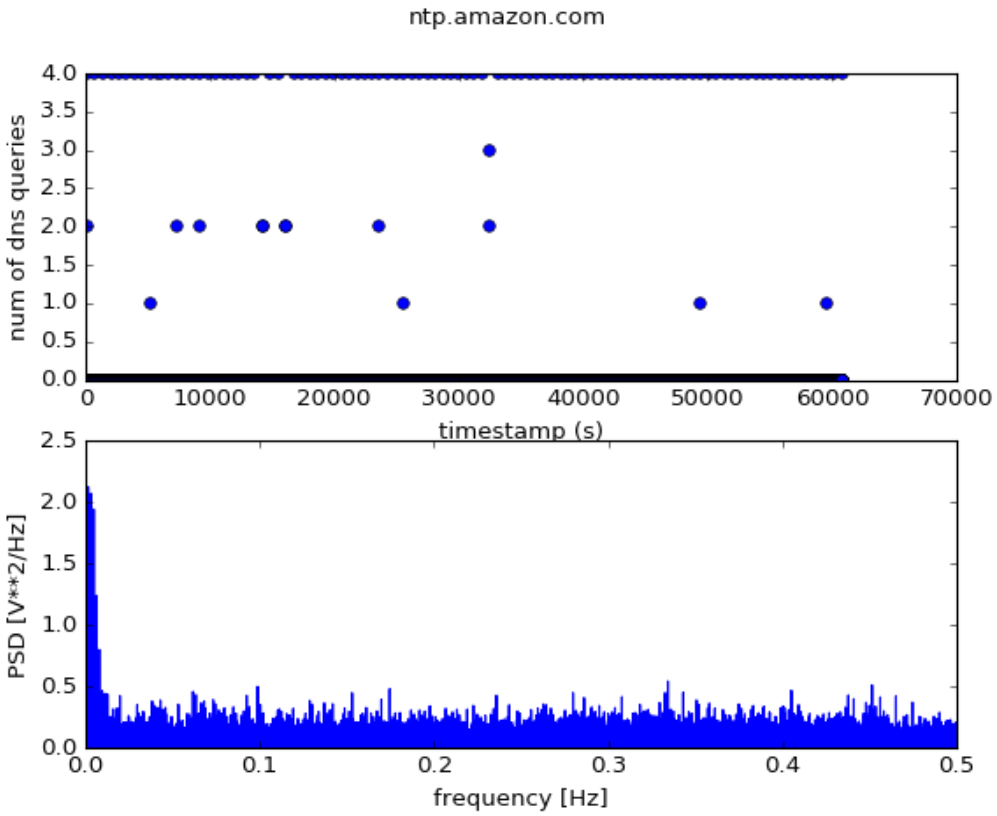


Amazon Echo (D02)

Domain	Num of queries	Period_freq (Hz)	Period (s)
*.north-america.pool.ntp.org	6+7+6+6 = 25		
amzdigitaldownloads.edgesuite.net	588 (bursty)		
device-metrics-us.amazon.com	133	301.58	0.003316
dp-449301NR._sftp-ssh._tcp.local … [*]	12		
esdk-ffl.spotify.com	1		
ntp-g7g.amazon.com	8		
ntp.amazon.com	405	633.125	0.001579

pindorama.amazon.com	16	4491.7	0.000223
pins.amazon.com	3		
softwareupdates.amazon.com	6		
spectrum.s3.amazonaws.com	3		
todo-ta-g7g.amazon.com	8		

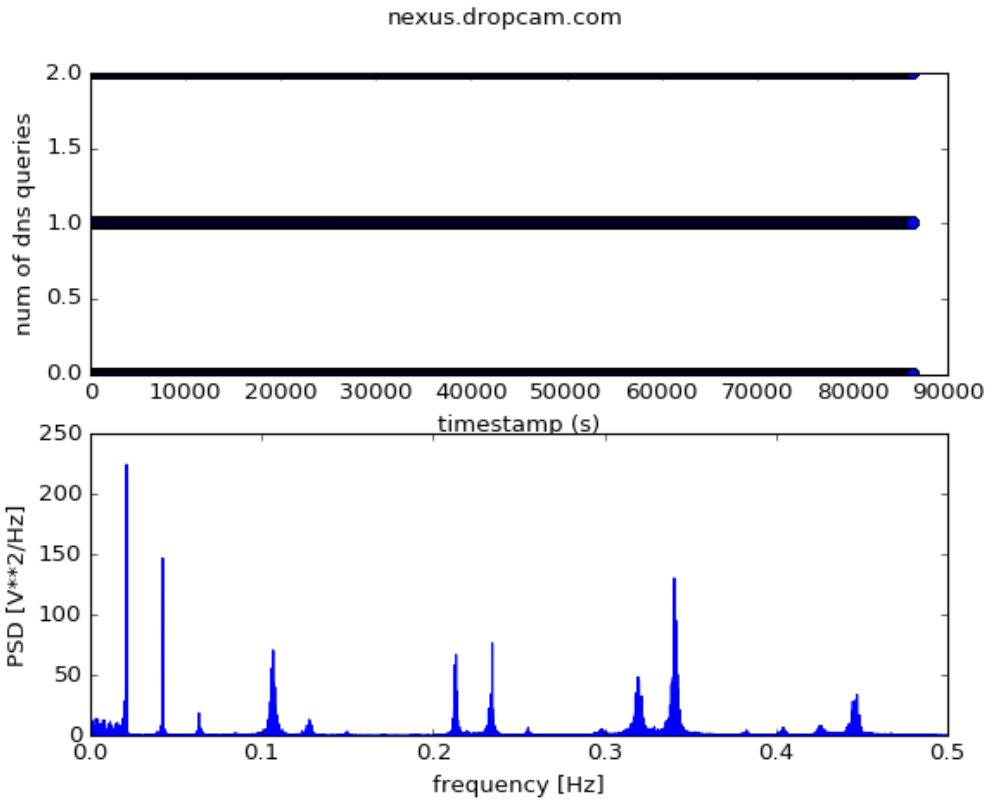




NEST DROPCAM

NestCam (D03a)

Domain	Num of queries	Period_freq (Hz)	Period (s)
nexus.dropcam.com	20454	0.021108	47.375
pool.ntp.org	41728	0.0211079	47.375



NestCam Active (D03b)

Domain	**Num of queries**	Period_freq (Hz)	Period (s)
nexus.dropcam.com	**2**		
oculus625-vir.dropcam .com	**2**		
pool.ntp.org	**4**		

- [pcap has lots of application data streams on port 443 but only 12 DNS related packets]

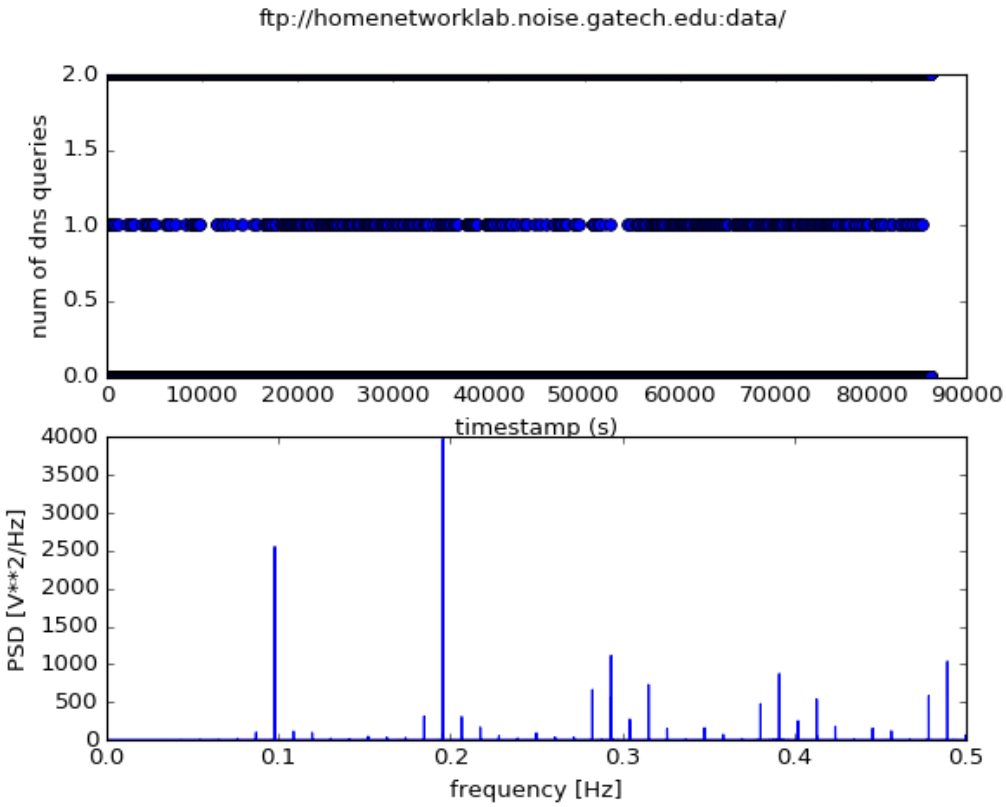
NestCam Active + View Stream (D03c)

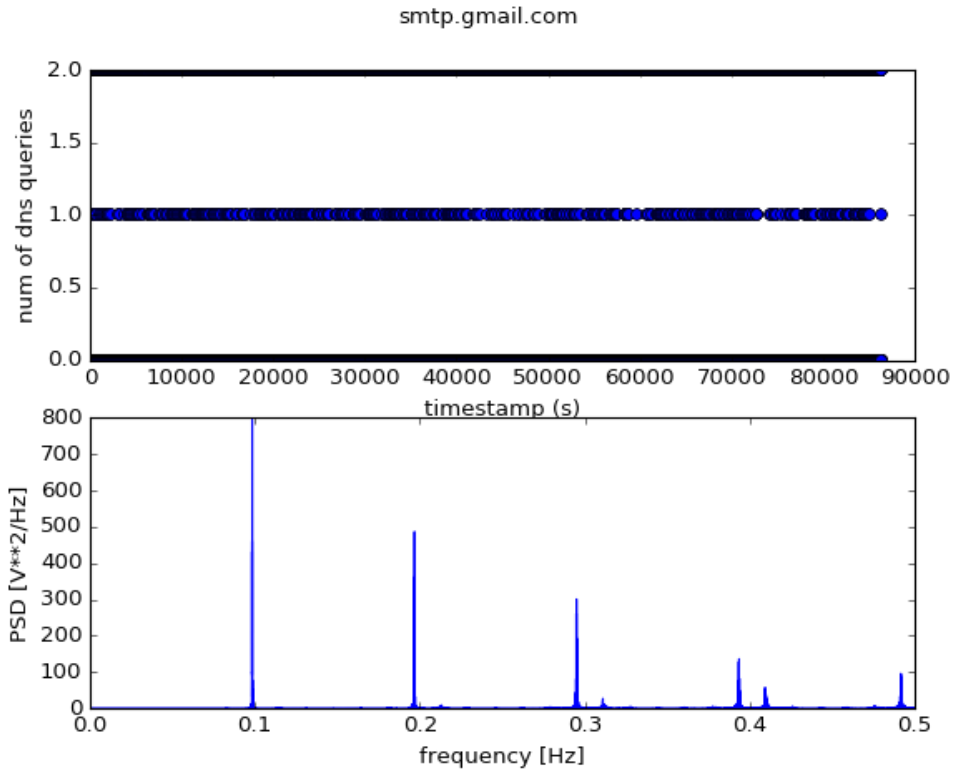
- shows same results - no DNS within the two hours when there is active traffic streaming
- (problem loading full 4.5 hr trace D03c - so split into 2 hr traces and load 2nd one)

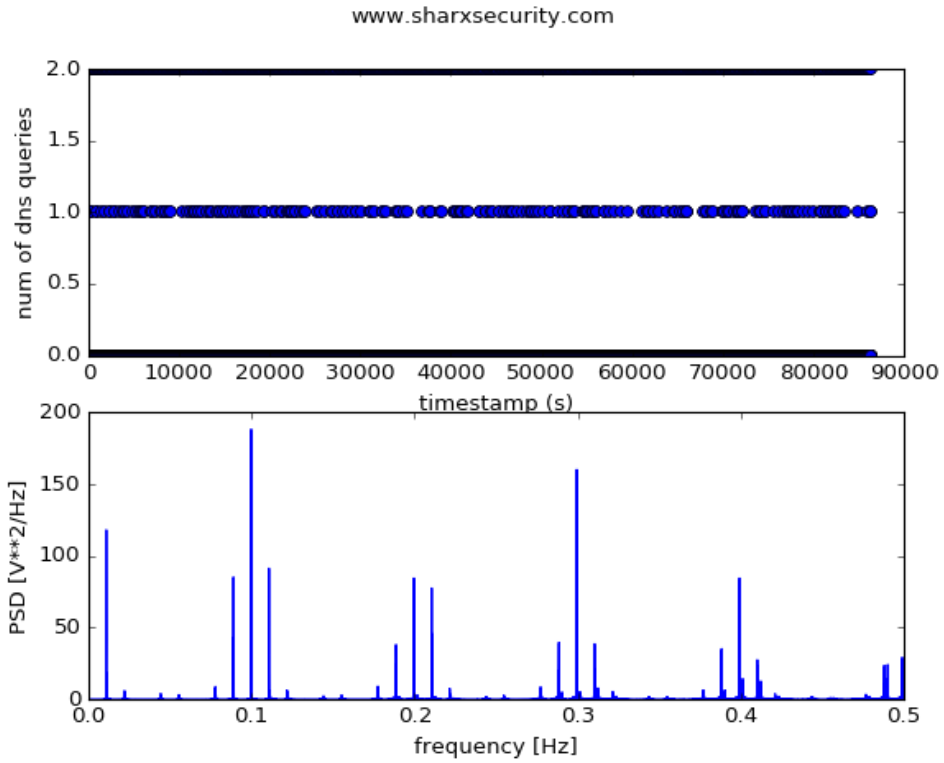
SHARX SECURITY CAMERA

SharxCam (D04a)

Domain	Num of queries	Period_freq (Hz)	Period (s)
ftp://homenetworklab.noise.gatech.edu:data/	16582	0.195646	5.111
smtp.gmail.com	16712	0.09832	10.17
time.nist.gov	16264	0.09628	10.386
www.sharxsecurity.com	5673	0.0997778	10.022




smtp.gmail.com
num of dns queries
timestamp (s)
PSD [V**2/Hz]
frequency [Hz]


www.sharxsecurity.com
num of dns queries
timestamp (s)
PSD [V**2/Hz]
frequency [Hz]

SharxCam Active (D04b)

Domain	Num of queries	Period_freq (Hz)	Period (s)
ftp://homenetworklab.noise.gatech.edu:data/	58269	0.076073	13.145
smtp.gmail.com	8569	0.19925	5.0187
time.nist.gov	2		
www.sharxsecurity.com	725	0.01662	60.133

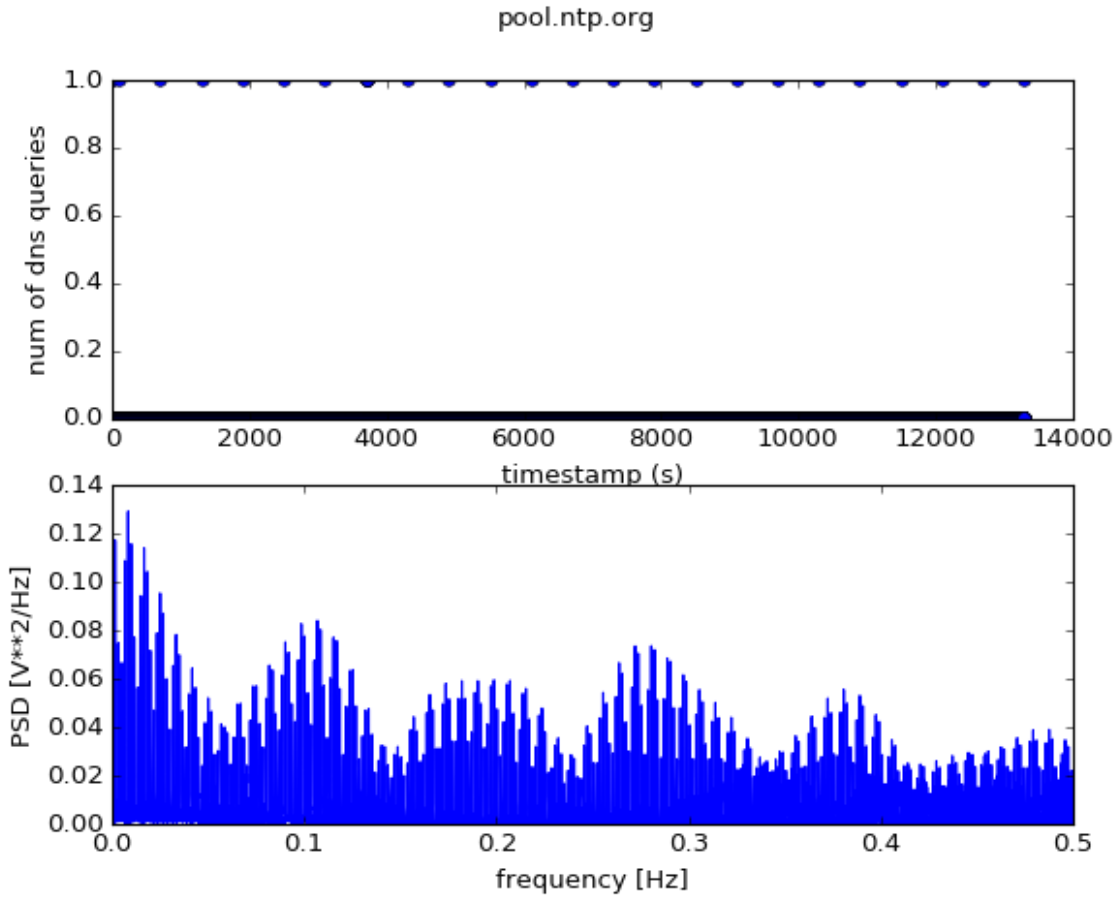
SharxCam Active + View Stream (D04c)

Domain	Num of queries	Period_freq (Hz)	Period (s)
ftp://homenetworklab.noise.gatech.edu:data/	9921	0.06487	15.415
smtp.gmail.com	1436	0.09946	10.054
www.sharxsecurity.com	120	0.016523	60.52

SMARTTHINGS

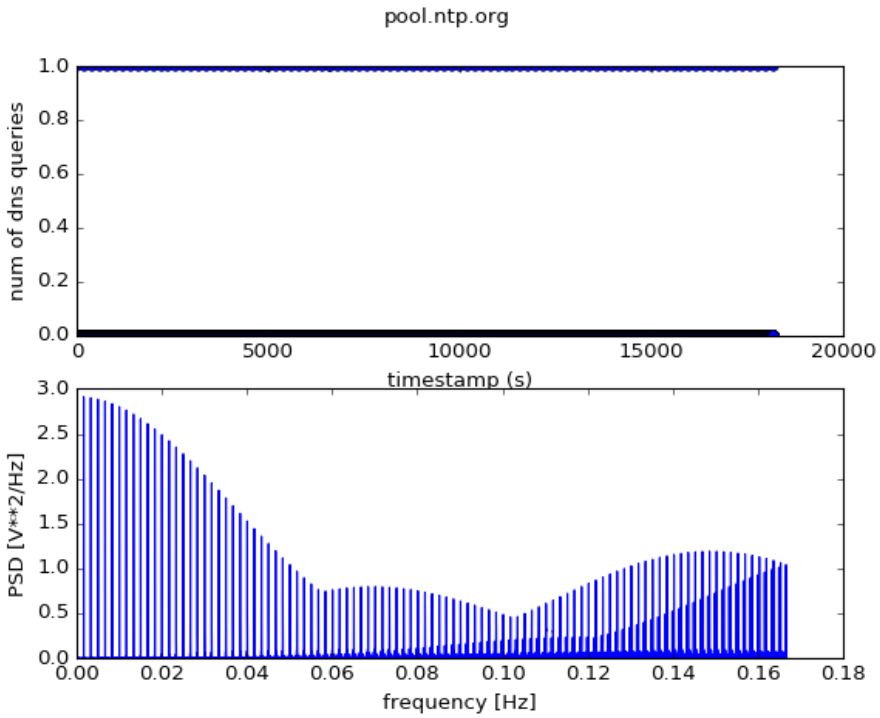
SmartThings alone (D05a)

Domain	Num of queries	Period_freq (Hz)	Period (s)
DC.connect.smartthings.com	4		
pool.ntp.org	30	0.008267	120.963



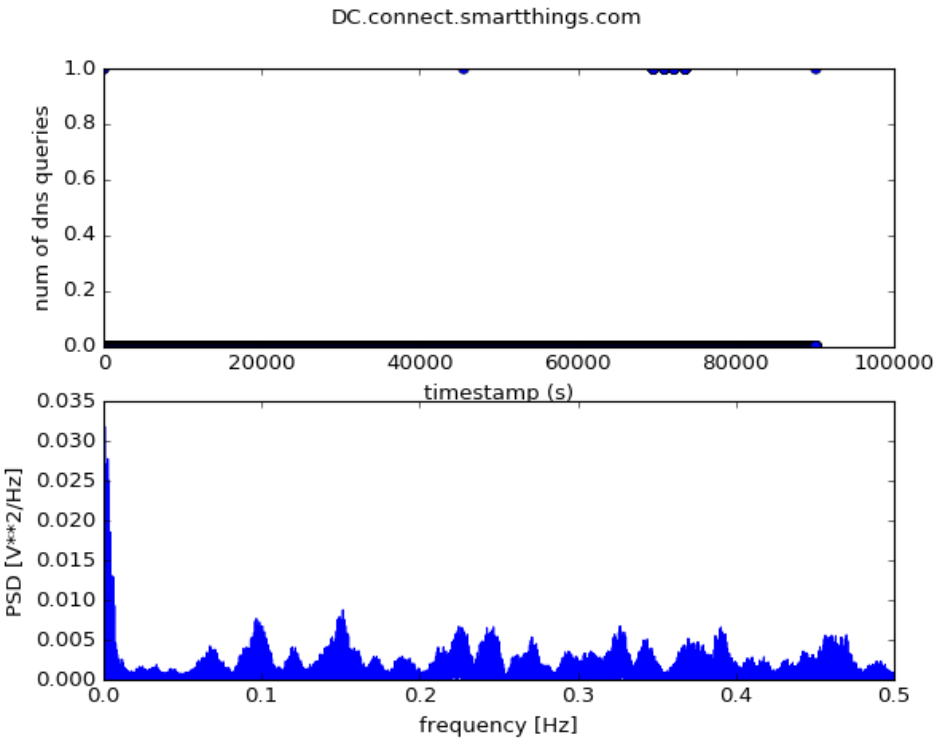
SmartThings + Door Sensor (D05b)

Domain	Num of queries	Period_freq (Hz)	Period (s)
DC.connect.smartthings.com	2		
pool.ntp.org	94	0.001651	605.66

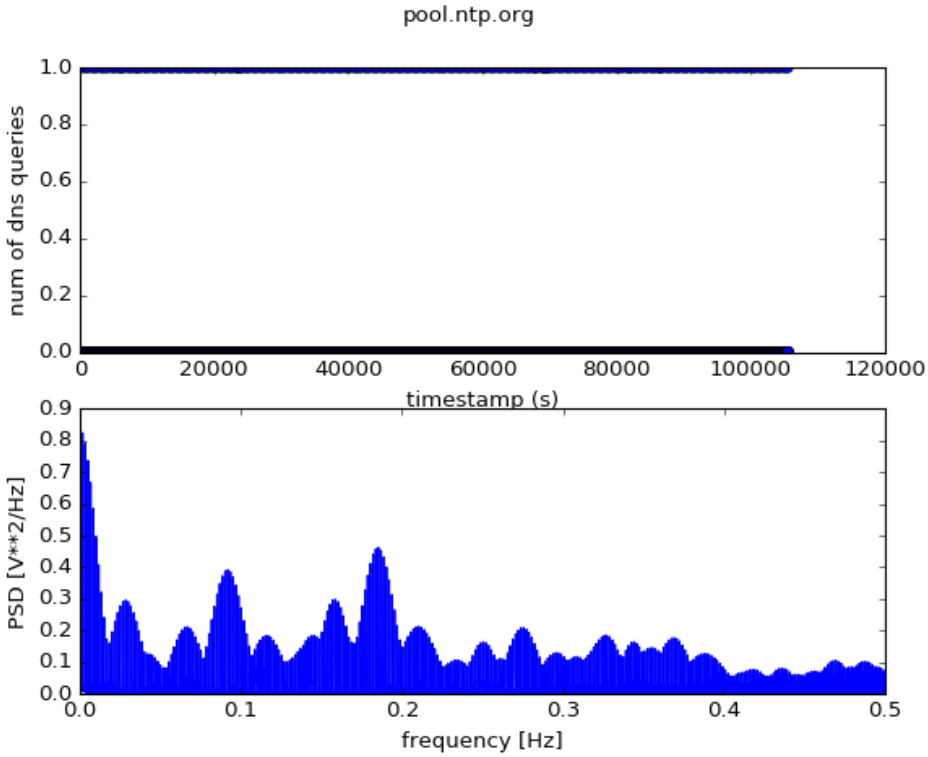


SmartThings + Smart Socket (D05c)

Domain	Num of queries	Period_freq (Hz)	Period (s)
DC.connect.smartthings.com	42	0.00071	1408.703
pool.ntp.org	210	0.001659	602.79



Clearly DC.smartthings.com is sporadic/bursty. We should detect this and avoid calculating period for such domains.



SmartThings + Door Sensor + Smart Socket (D05d)

Domain	Num of queries	Period_freq (Hz)	Period (s)
DC.connect.smartthings.com	25		
pool.ntp.org	115	0.001650	605.867