SRUM forensics

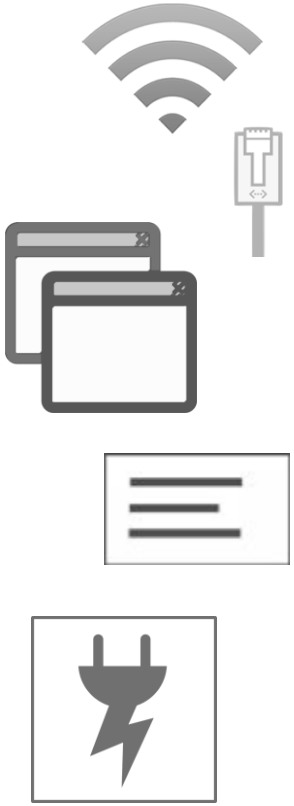
Yogesh Khatri
Champlain College

What is SRUM?

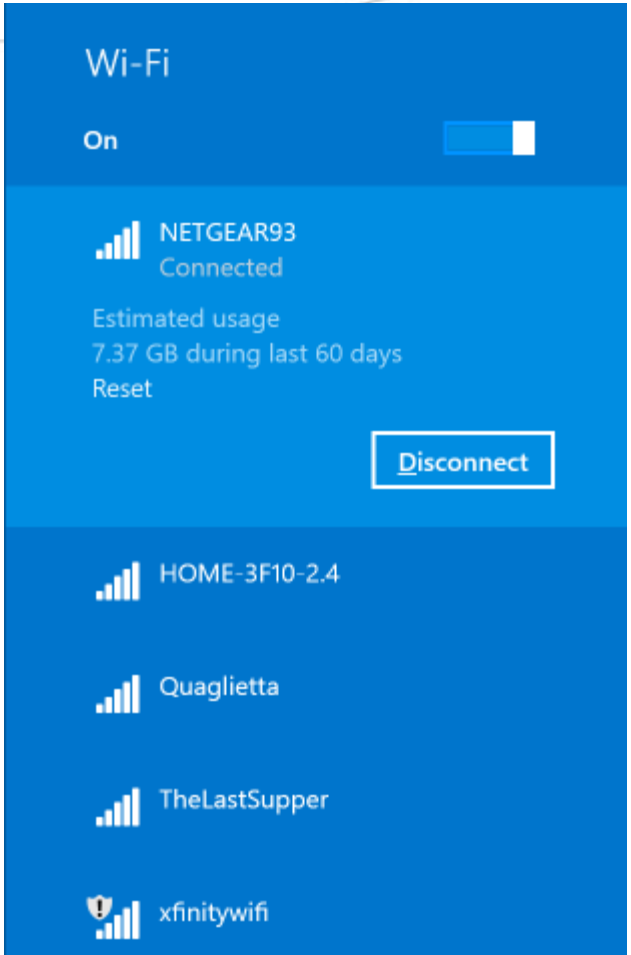
- System Resource Usage Monitor
  - First seen in Windows 8
  - Part of Diagnostic Policy Service
- Technology that monitors desktop application programs, services, windows apps and network connections
- Maintains database of historical activity!

System Resource Usage Monitor

- Network Connectivity
- Network Data usage
- Application Resource usage
- Windows push notifications
- Energy usage



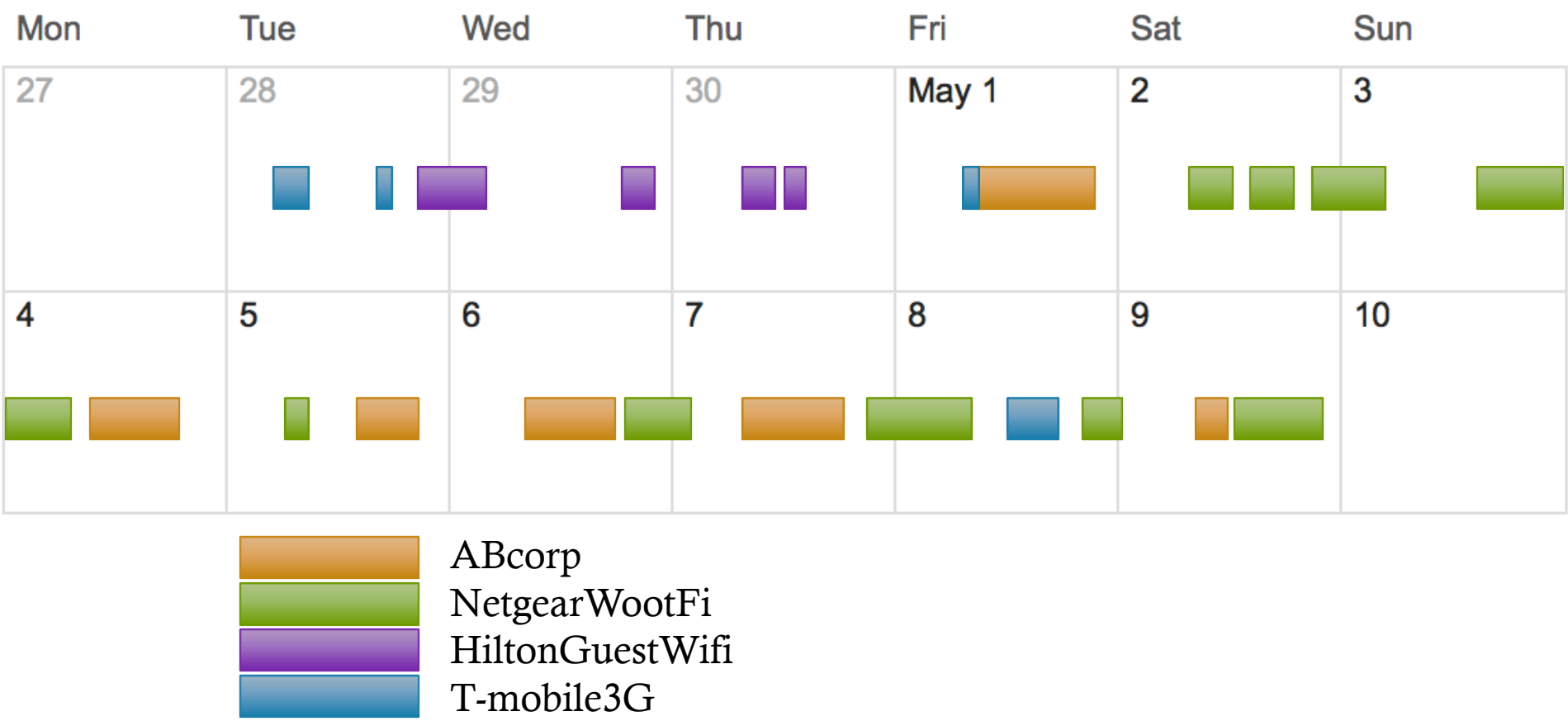
Network Connectivity & usage



Network Connectivity

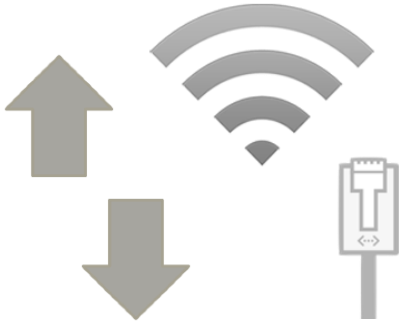
- SRUM tracks periods of network connectivity (since 8.1)
- Items tracked
  - Interface Type & ID
  - Network Profile ID
  - Time connection established
  - Length of time connected

Network connectivity tracking



Network Usage

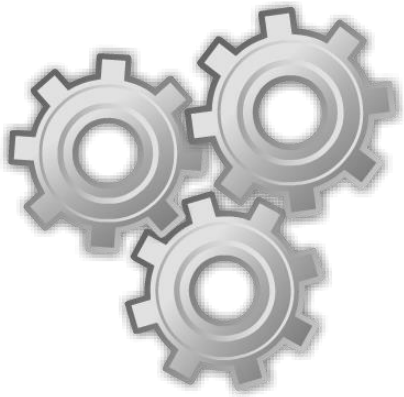
- Information available
  - Application/Service/App consuming data
    - User SID
  - Bytes Uploaded & Downloaded
  - Interface Type & ID
  - Network Profile ID



- NOT available
  - Endpoint info (IP addresses, Port numbers)
  - Specific data information (what was downloaded?)

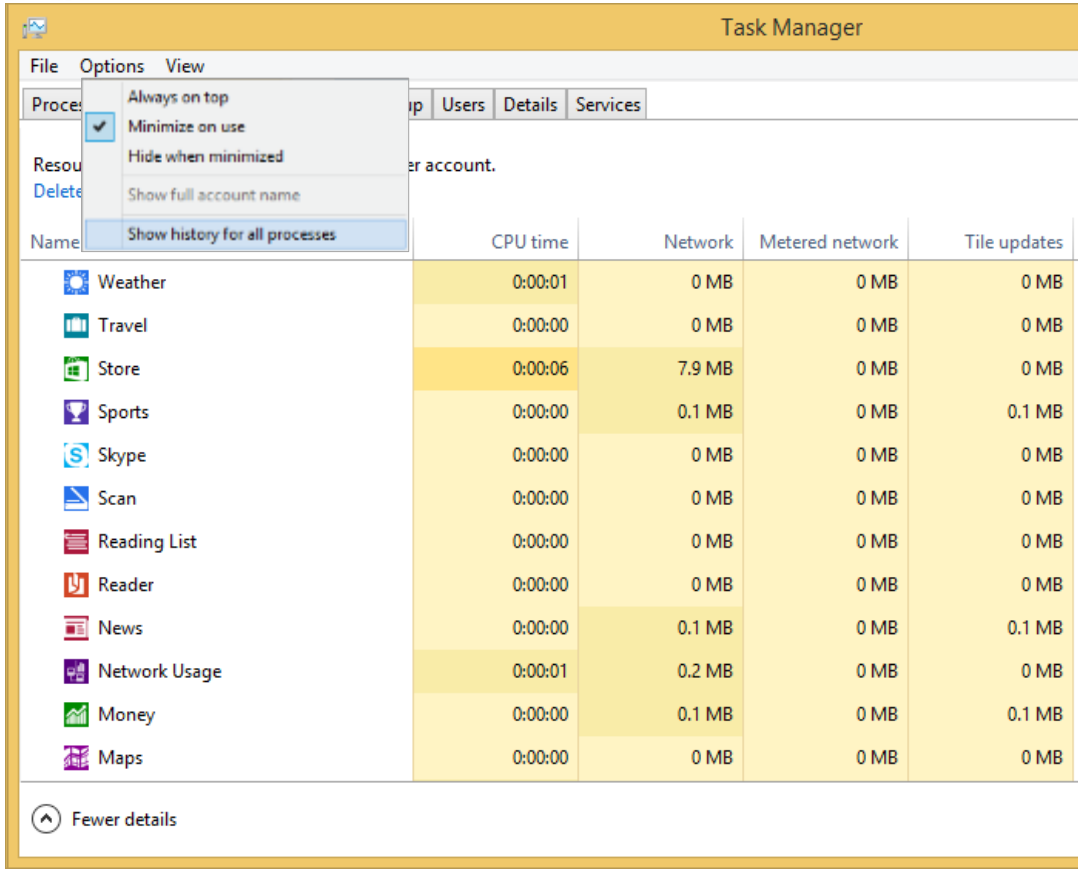
Application Resource tracking

- Process Information
  - CPU cycles
  - Context switches
  - I/O bytes read/written
  - Number of read operations
  - Number of write operations
  - Number of Flushes
- User Information
  - SID of user who launched program
- NOT available
  - Memory, Threads, Handles, Cache or Kernel info



App History

- Both App & Desktop Application history
- To view Desktop Application history
  - View → Show history for all processes
- 'Uninstalled Processes' are all programs no longer on disk (in their original locations)



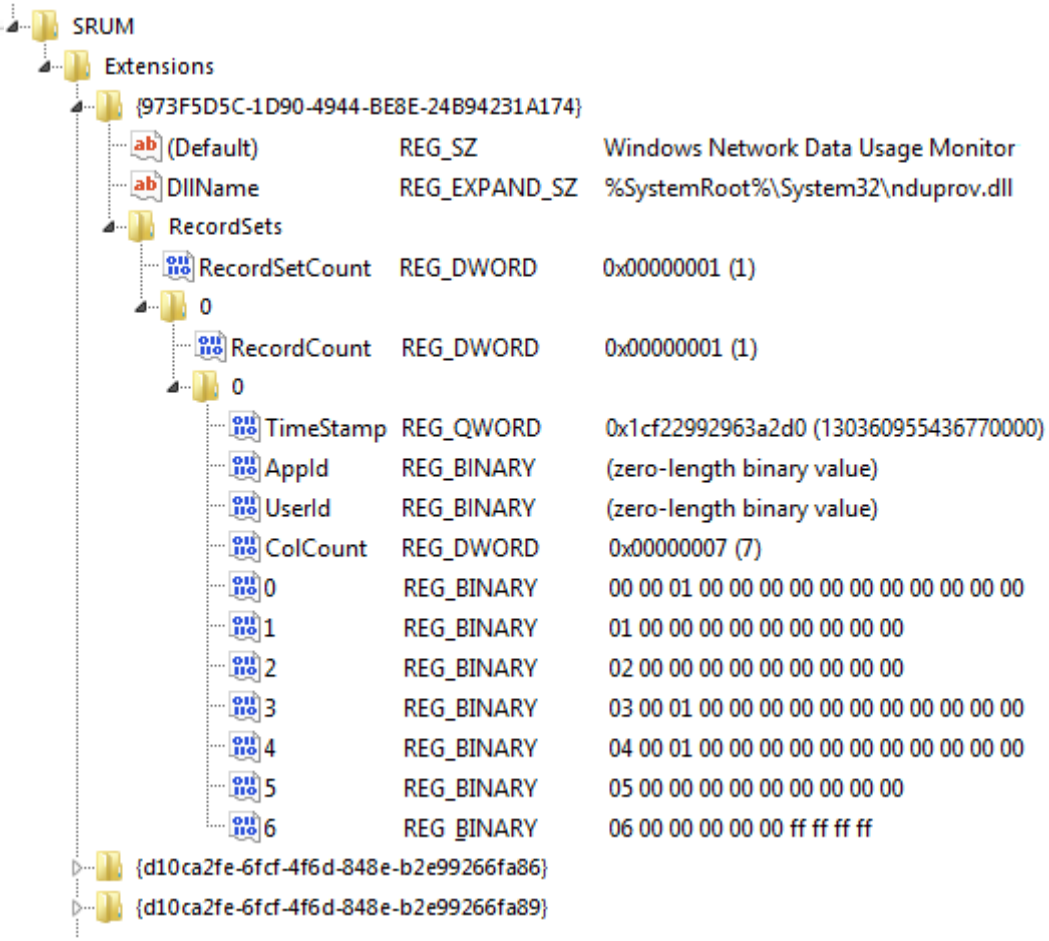
Data Collection

- Written once every hour and at shutdown
- Extensions monitor and collect data

SRUM Extension	GUID	DLL in System32
Windows Network Data Usage Monitor	{973F5D5C-1D90-4944-BE8E-24B94231A174}	nduprov.dll
Windows Push Notifications (WPN) Provider	{d10ca2fe-6fcf-4f6d-848e-b2e99266fa86}	wpnsruprov.dll
Application Resource Usage Provider	{d10ca2fe-6fcf-4f6d-848e-b2e99266fa89}	appsruprov.dll
Windows Network Connectivity Usage Monitor	{DD6636C4-8929-4683-974E-22C046A43763}	ncuprov.dll
Energy Usage Provider	{fee4e14f-02a9-4550-b5ce-5fa2da202e37}	energyprov.dll

SRUM data in registry

- Registry is temporary location for holding data
  - Data is periodically moved to SRUDB.dat
- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SRUM\Extensions



SRUM Database

- ESE database on disk
  - C:\Windows\System32\sru\SRUDB.dat
  - ESE is Extensible Storage Engine
    - Windows Updates, Active Directory, Windows Search, IE11, ..

Database Table Name	Description
{DD6636C4-8929-4683-974E-22C046A43763}	Network Connectivity data
{D10CA2FE-6FCF-4F6D-848E-B2E99266FA89}	Application Resource usage data
{973F5D5C-1D90-4944-BE8E-24B94231A174}	Network usage data
{D10CA2FE-6FCF-4F6D-848E-B2E99266FA86}	Windows Push Notification data
{FEE4E14F-02A9-4550-B5CE-5FA2DA202E37}	Energy usage data
{FEE4E14F-02A9-4550-B5CE-5FA2DA202E37}LT	Energy usage data

Raw data
Network data usage

	A	B	C	D	E	F	G	H	I
1	AutoIncId	TimeStamp	AppId	UserId	InterfaceLuid	L2ProfileId	L2ProfileFlags	BytesSent	BytesRecvd
2	441	(0x40e49060 0x00000000)	80	69	19984723363233792	268435458	0	554	392
3	442	(0x40e49060 0x00000000)	5	4	19984723363233792	268435458	0	256	0
4	443	(0x40e49060 0x00000000)	65	4	19984723363233792	268435458	0	1080	0
5	444	(0x40e49060 0x00000000)	66	37	19984723363233792	268435458	0	213	0
6	445	(0x40e49060 0x00000000)	1	2	19984723363233792	268435458	0	7327	2287
7	446	(0x40e49060 0x00000000)	67	37	19984723346456576	268435457	0	38532	22639
8	447	(0x40e49060 0x00000000)	5	4	19984723346456576	268435457	0	39733	74857
9	448	(0x40e49060 0x00000000)	227	37	19984723346456576	268435457	0	2720	17322
10	449	(0x40e49060 0x00000000)	60	37	19984723346456576	268435457	0	17885	94171
11	450	(0x40e49060 0x00000000)	64	30	19984723346456576	268435457	0	923	1044
12	451	(0x40e49060 0x00000000)	80	69	19984723346456576	268435457	0	146179	1836276
13	452	(0x40e49060 0x00000000)	62	4	19984723346456576	268435457	0	1377143	21685093
14	453	(0x40e49060 0x00000000)	66	37	19984723346456576	268435457	0	22929	0
15	454	(0x40e49060 0x00000000)	59	30	19984723346456576	268435457	0	12294	22818
16	455	(0x40e49060 0x00000000)	65	4	19984723346456576	268435457	0	79184	2512
17	456	(0x40e49060 0x00000000)	73	69	19984723346456576	268435457	0	2395	7089
18	457	(0x40e49060 0x00000000)	1	2	19984723346456576	268435457	0	3525360	68250284
19	458	(0x40e49060 0x00000000)	224	69	19984723346456576	268435457	0	4035	97156
20	459	(0x40e49060 0x00000000)	320	4	19984723346456576	268435457	0	8159	32586
21	460	(0x40e49060 0x00000000)	76	4	19984723346456576	268435457	0	16524	11214
22	461	(0x40e49060 0x00000000)	61	4	19984723346456576	268435457	0	1436540	43763698
23	462	(0x40e49060 0x00000000)	224	4	19984723346456576	268435457	0	640	469
24	463	(0x40e49060 0x00000000)	228	37	19984723346456576	268435457	0	3070	15070
25	464	(0x40e49060 0x00000000)	71	72	19984723346456576	268435457	0	6456	4503

Data needing interpretation/conversion

- Timestamps are in UTC in OLE format (64 bits) and FILETIME format (64 bits)
- Network interfaces are specified as InterfaceLuid (NET_LUID)

```
typedef union _NET_LUID {
  ULONG64 Value;
  struct {
    ULONG64 Reserved  :24;
    ULONG64 NetLuidIndex  :24;
    ULONG64 IfType  :16;
  } Info;
} NET_LUID, *PNET_LUID;
```

IfType can be WiFi (802.11), Ethernet, ATM, 4G or one of several other values

Resolving network profile from L2ProfileId field

- Lookup HKLM\SOFTWARE\Microsoft\WlanSvc\Interfaces\{*Int*

RegistryViewer

File Extras Help

Interfaces
- {112FCFE3-E221-4DBF-A056-B4FECC4BB7E4}
- {25A1ED24-171B-4358-9D13-31C76F8AC6E3}
- {2ABAAADD-58D0-4F33-96A4-A9ACBF165433}
- {32FFE5DA-6C69-4CD5-B844-FC0ACB6DCAB2}
- {706D4E8B-8487-4739-B5C1-34B35710B50F}
- {7B75EA06-CE7B-43BC-9B0E-A6A58BF716F1}
  - Profiles
    - {1E9BA135-2B19-4BFF-BF9E-68291ECB021B}
      - MetaData

Value	Type	Length	Data
Flags	REG_DWORD	4	0 (0x00000000)
ProfileIndex	REG_DWORD	4	268435457 (0x10000001)

Value	Type	Length
All User Profile Security Descriptor	REG_BINARY	378
Channel Hints	REG_BINARY	84
CreatorSid	REG_BINARY	28
Nla	REG_BINARY	4
succeeded	REG_BINARY	4

	0001 0203 0405 0607 0809 0A0B 0C0D	0123456789ABCD
0x00	0900 0000 4E45 5447 4541 5239 3300	....NETGEAR93.
0x0E	0000 0000 0000 0000 0000 0000 0000	.....
0x1C	0000 0000 0000 0000 DF07 0600 0100	.....ß.....
0x2A	0F00 0E00 0C00 0A00 B300 0700 0000	.....³.....
0x38	0B00 0000 0700 0000 0600 0000 0000	.....
0x46	0000 0000 0000 0000 0000 0000 0000	.....

Reading SRUM data

1. Use libesedb (https://github.com/libyal/libesedb) to convert ESE database tables to csv format
2. Use script available at www.swiftforensics.com to
   - Resolve Foreign keys, parse InterfaceLuids and timestamps from tables
   - Parse Network profiles from registry
   - Read and parse SRUM data from registry

Parsed/Resolved data
Network data usage

A	B	C	D	E	F	G	H	I	J	K
AutoIncId	TimeStamp	AppId	UserId	If Type	If Id	L2ProfileId	BytesSent	BytesRecvd	AppName	NetworkProfile
441	4/20/15 20:00	\device\hard	S-1-5-21-366	IEEE80211	1	268435458	554	392	chrome.exe	NETGEAR93
442	4/20/15 20:00	System	S-1-5-18	IEEE80211	1	268435458	256	0	System	NETGEAR93
443	4/20/15 20:00	System\IPv6	S-1-5-18	IEEE80211	1	268435458	1080	0	IPv6 Control Message	NETGEAR93
444	4/20/15 20:00	Dhcp	S-1-5-19	IEEE80211	1	268435458	213	0	Dhcp	NETGEAR93
445	4/20/15 20:00			IEEE80211	1	268435458	7327	2287		NETGEAR93
446	4/20/15 20:00	SSDPSRV	S-1-5-19	IEEE80211	0	268435457	38532	22639	SSDPSRV	NETGEAR93
447	4/20/15 20:00	System	S-1-5-18	IEEE80211	0	268435457	39733	74857	System	NETGEAR93
448	4/20/15 20:00	wcncsvc	S-1-5-19	IEEE80211	0	268435457	2720	17322	wcncsvc	NETGEAR93
449	4/20/15 20:00	\device\hard	S-1-5-19	IEEE80211	0	268435457	17885	94171	dashost.exe	NETGEAR93
450	4/20/15 20:00	NlaSvc	S-1-5-20	IEEE80211	0	268435457	923	1044	NlaSvc	NETGEAR93
451	4/20/15 20:00	\device\hard	S-1-5-21-366	IEEE80211	0	268435457	146179	1836276	chrome.exe	NETGEAR93
452	4/20/15 20:00	wuauserv	S-1-5-18	IEEE80211	0	268435457	1377143	21685093	wuauserv	NETGEAR93
453	4/20/15 20:00	Dhcp	S-1-5-19	IEEE80211	0	268435457	22929	0	Dhcp	NETGEAR93
454	4/20/15 20:00	Dnscache	S-1-5-20	IEEE80211	0	268435457	12294	22818	Dnscache	NETGEAR93
455	4/20/15 20:00	System\IPv6	S-1-5-18	IEEE80211	0	268435457	79184	2512	IPv6 Control Message	NETGEAR93
456	4/20/15 20:00	\device\hard	S-1-5-21-366	IEEE80211	0	268435457	2395	7089	explorer.exe	NETGEAR93
457	4/20/15 20:00			IEEE80211	0	268435457	3525360	68250284		NETGEAR93
458	4/20/15 20:00	CryptSvc	S-1-5-21-366	IEEE80211	0	268435457	4035	97156	CryptSvc	NETGEAR93
459	4/20/15 20:00	iphlpsvc	S-1-5-18	IEEE80211	0	268435457	8159	32586	iphlpsvc	NETGEAR93
460	4/20/15 20:00	DsmSvc	S-1-5-18	IEEE80211	0	268435457	16524	11214	DsmSvc	NETGEAR93
461	4/20/15 20:00	BITS	S-1-5-18	IEEE80211	0	268435457	1436540	43763698	BITS	NETGEAR93
462	4/20/15 20:00	CryptSvc	S-1-5-18	IEEE80211	0	268435457	640	469	CryptSvc	NETGEAR93
463	4/20/15 20:00	EventSystem	S-1-5-19	IEEE80211	0	268435457	3070	15070	EventSystem	NETGEAR93
464	4/20/15 20:00	\device\hard	S-1-5-21-366	IEEE80211	0	268435457	6456	4503	daemonu.exe	NETGEAR93

Forensic Uses

SRUM Data

User-Process mapping

- Which user launched the process?

Network statistics

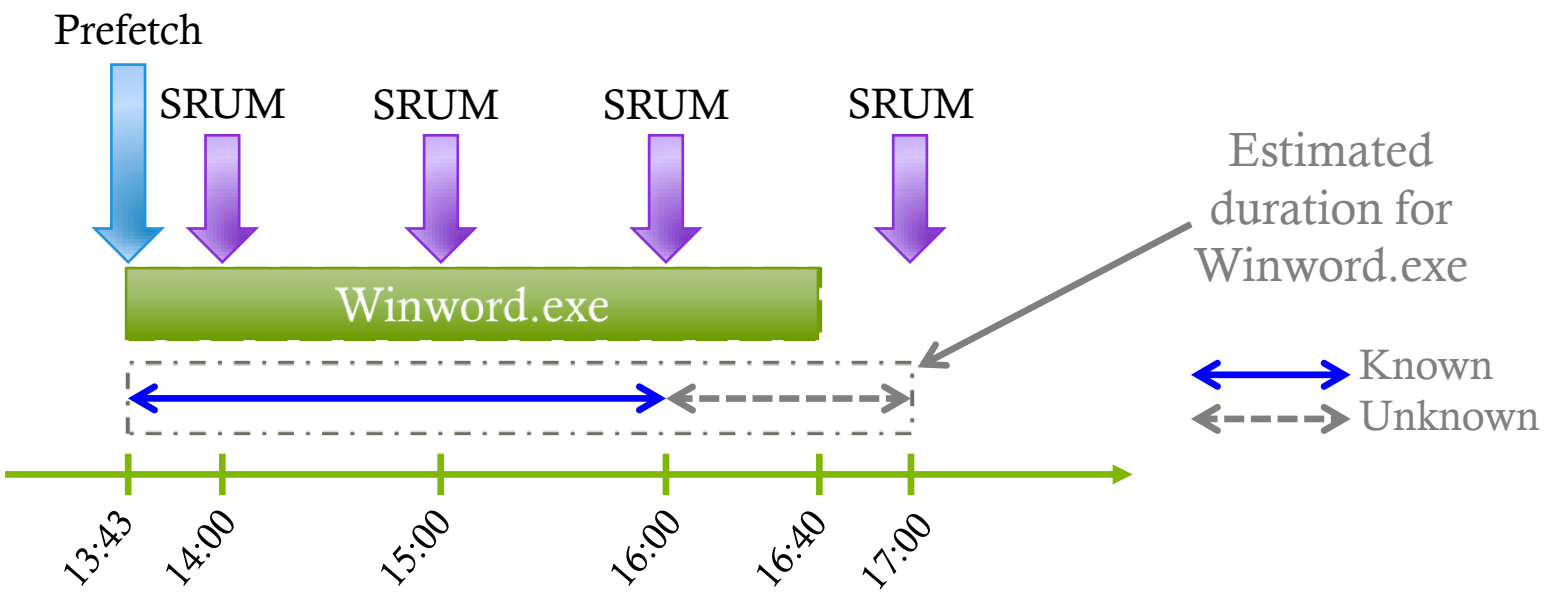
- Data upload/download per network and per process

Application run times can be estimated

Deleted/Uninstalled/External program tracking

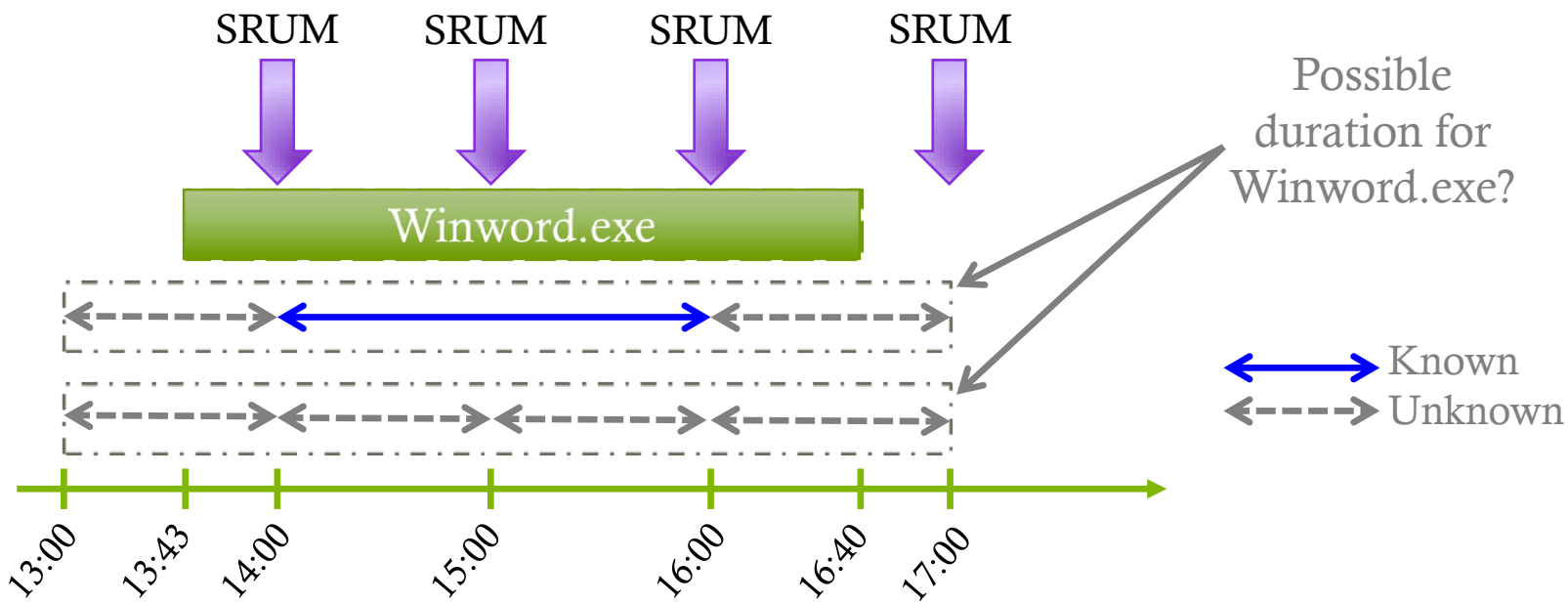
Estimate Process Run time

- Prefetch file records start time of process, not duration



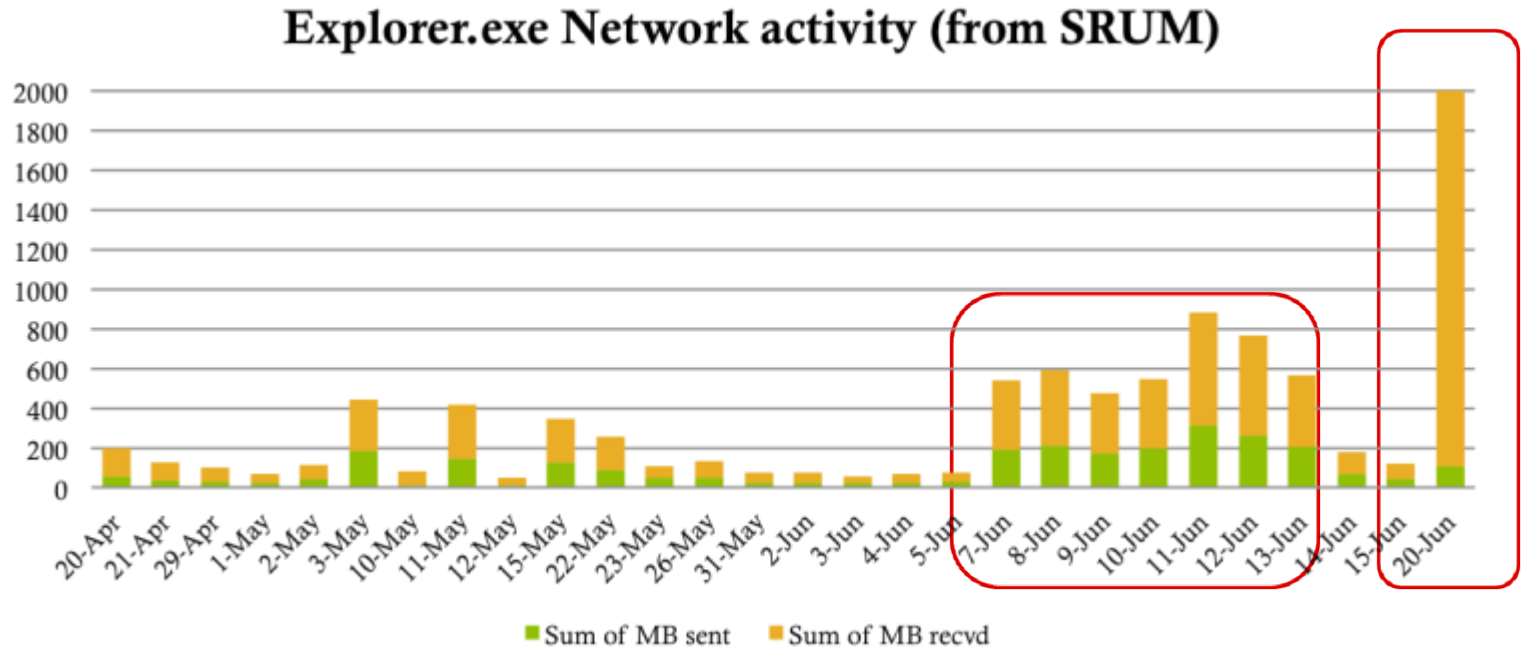
Estimate Process Run time

- Prefetch only retains last 8 start times, no record of prior runs
  - SRUM can tell you if an app was run or not



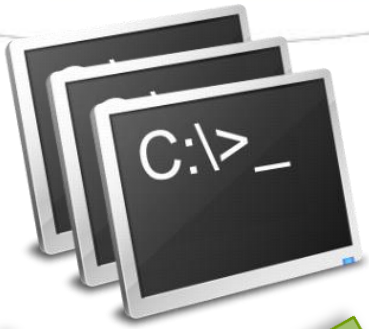
Typical Data Theft scenario

- Employee downloads a lot of data from the intranet just before leaving the company



Investigate Program usage

Program run approx. timespan (precision is one hour)



Identify User who launched program

Identify network & Profile used

Get Data statistics – How much data uploaded & downloaded?

Detailed Process Stats
CPU cycles
Context switches
I/O bytes read/written
Number of read operations
Number of write operations
Number of Flushes

Questions?

- Thanks for listening!
- Link to paper – Forensic Implications of SRUM in windows 8
  - http://www.sciencedirect.com/science/article/pii/S1742287615000031

Contact info:

www.swiftforensics.com

yogesh@swiftforensics.com