NETRESEC

SCADA Network Forensics

Erik Hjelmvik
<erik.hjelmvik[at]netresec.com>

Stockholm, Sweden 2014-10-22

NetworkMiner packet analyzer

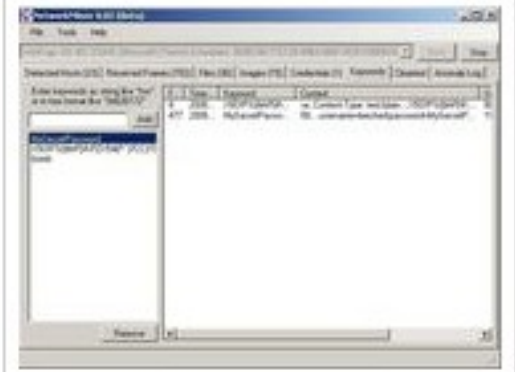
The Network Forensics Tool

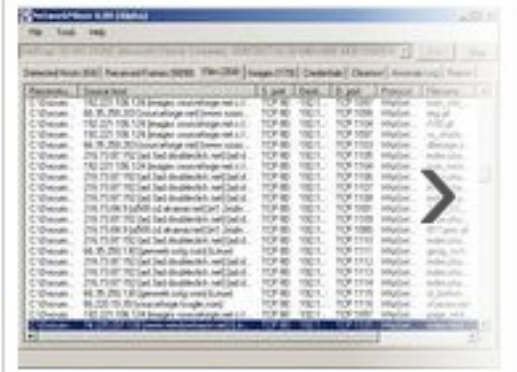
Brought to you by: hjelmvik

★ 5.0 Stars (18)

2 263 Downloads (This Week)

Last Update: 2014-06-24





Havex RAT

Malware: Havex RAT

Threat Actor: Dragonfly / Energetic Bear / Crouching Yeti

CrowdStrike:

"ENERGETIC BEAR is an adversary [...] with a primary focus on the energy sector."

"ENERGETIC BEAR is operating out of Russia, or at least on behalf of Russia-based interests, and it is possible that their operations are carried out with the sponsorship or knowledge of the Russian state."

CROWDSTRIKE

Havex RAT

Malware: Havex RAT

Threat Actor: Dragonfly / Energetic Bear / Crouching Yeti

Kaspersky:

"The Crouching Yeti actor performed a massive surveillance operation targeting strategic victims"

Targeted sectors include:

- Industrial/machinery
- Manufacturing
- Pharmaceutical
- [...]

"Energetic Bear/Crouching Yeti is an actor involved in several Advanced Persistent Threat (APT) campaigns"

Trojanized ICS Installers

Symantec:

"Three different ICS equipment providers were targeted and malware was inserted into the software bundles they had made available for download on their websites."


If the names of the vendors that unwittingly spread Havex were made public, the wide coverage would likely reach most of the affected asset owners.
Dale Peterson
Smart ICS Security guy, former NSA geek

Havex Trojan #1

- Symantec: "a product used to provide VPN access to programmable logic controller (PLC) type devices."
- Their site was compromised for ten days beginning in January 2014 when approximately 250 copies of the malicious software were downloaded

Havex Trojan #1

Product:
Talk2M eCatcher 4.0.0.13073

Company:
eWON

MD5:
eb0dacdc8b346f44c8c370408bad4306

SHA256:
70103c1078d6eb28b665a89ad0b3d11c1cbca61a05a18f87f6a16c79b501dfa9

Havex Trojan #2

- Symantec: "European manufacturer of specialist PLC type devices."
- "the Trojanized software was available for download for at least six weeks in June and July 2013."

Havex Trojan #2

Product:
Swiss Ranger
1.0.14.706
(libMesaSR)

Company:
MESA Imaging

MD5:
e027d4395d9ac9cc
980d6a91122d2d83

SHA256:
398a69b8be2ea2b4
a6ed23a55459e046
9f657e6c7703871f
63da63fb04cefe90

Havex Trojan #3

- Symantec: "European company which develops systems to manage wind turbines, biogas plants, and other energy infrastructure."
- Trojan available during ten days in April 2014

Havex Trojan #3.1

Product:
mbCONFTOOL
v1.0.1

Company: MB
Connect Line GmbH

MD5:
0a9ae7fdcd9a9fe0
d8c5c106e8940701

SHA256:
c32277fba70c82b2
37a86e9b542eb11b
2b49e4995817b7c2
da3ef67f6a971d4a

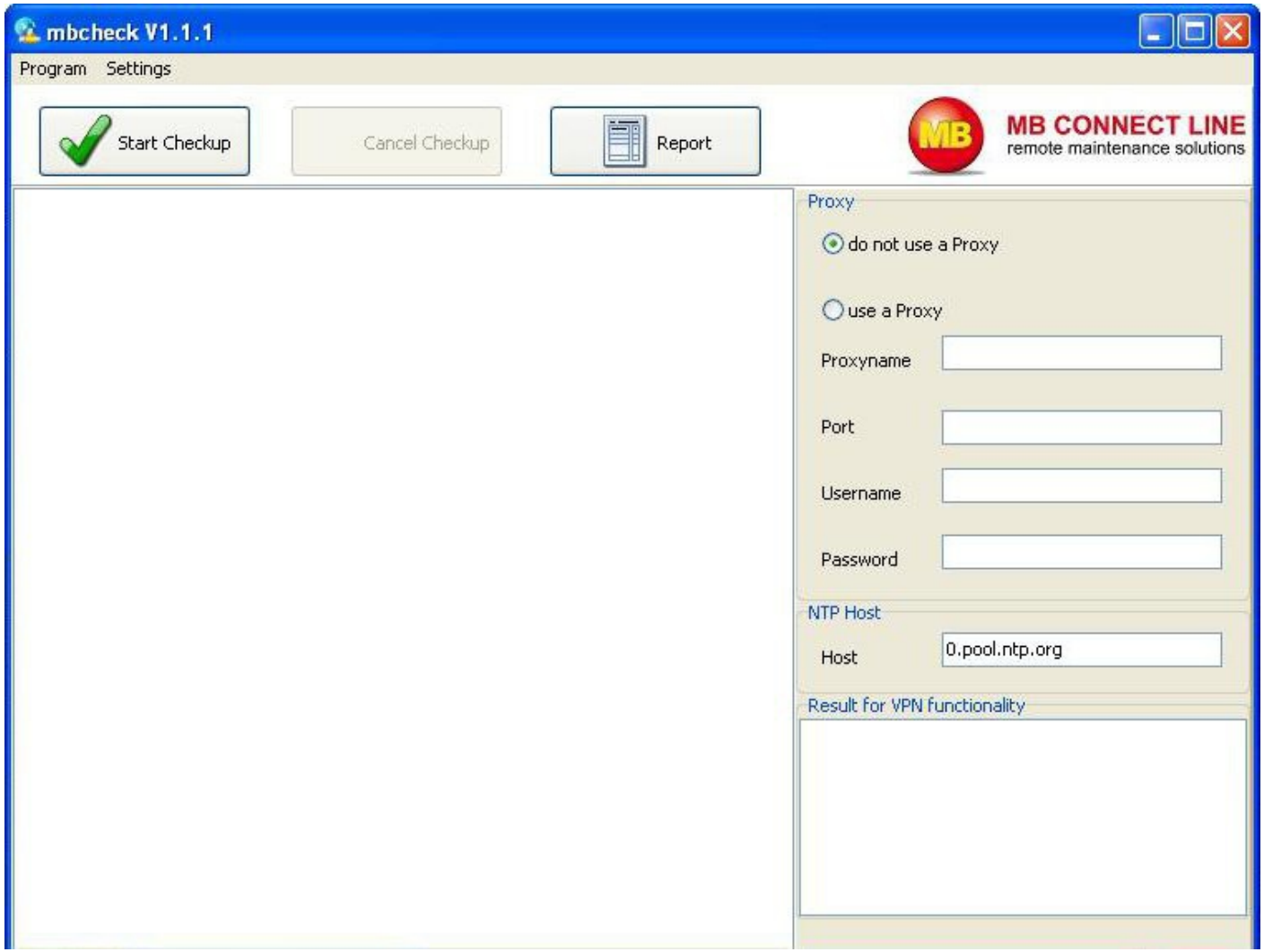
Havex Trojan #3.2

Product:
mbCHECK
v1.1.1

Company: MB
Connect Line GmbH

MD5:
1d6b11f85debdda2
7e873662e721289e

SHA256:
0b74282d9c03affb
25bbecf28d5155c5
82e246f0ce21be27
b75504f1779707f5



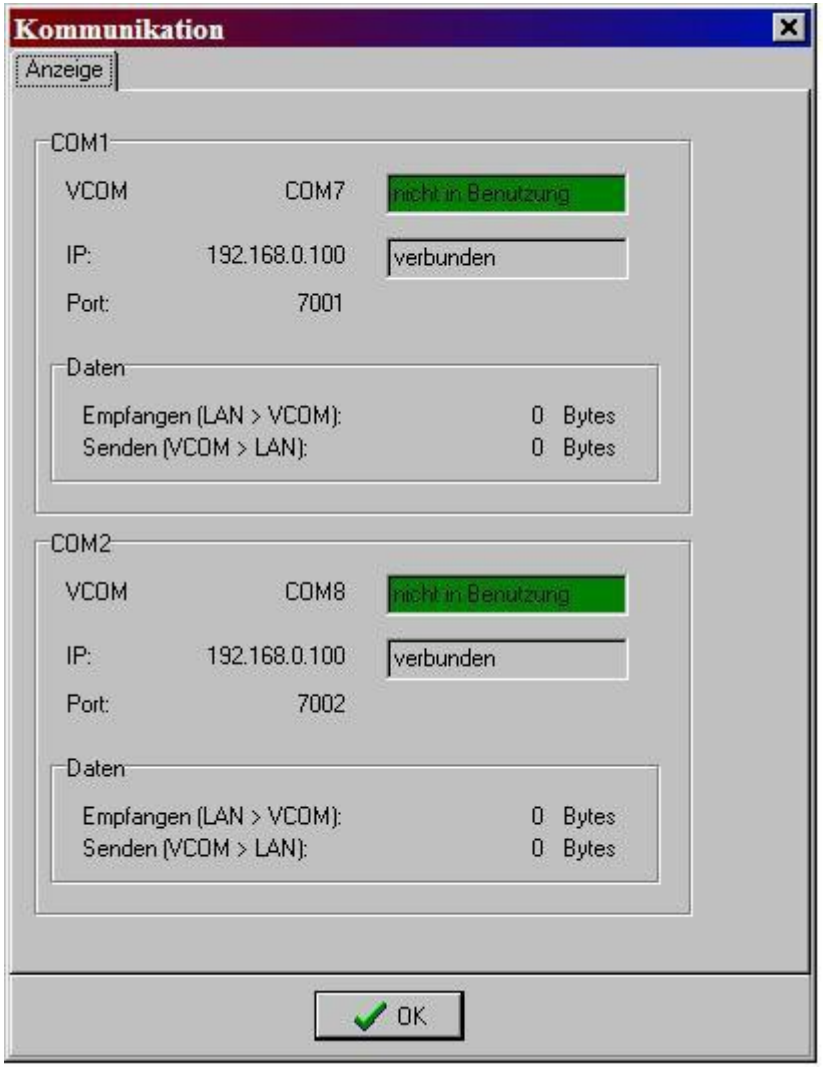
Havex Trojan #3.3

Product:
VCOM_LAN2
<unknown version>

Company: MB
Connect Line GmbH

MD5:
<unknown hash>

SHA256:
<unknown hash>




We don't know how many other SCADA systems have been compromised because they don't really have **cyber forensics**.
(Joe Weiss, 2012)
Joe Weiss
Very important Control System Security guy

Cyber Forensics

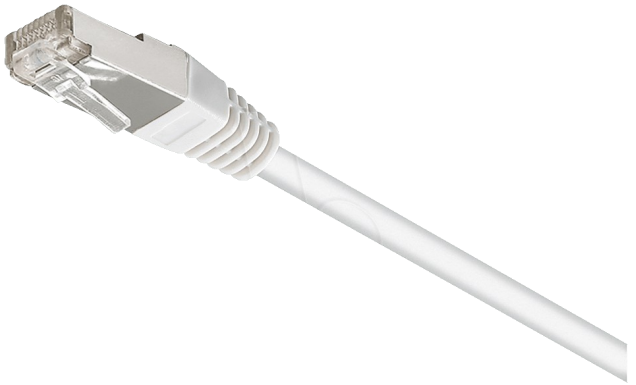
\ˈsī-bər fə-ˈren-siks\

Digital Forensics

Disk Forensics	Memory Forensics	Network Forensics

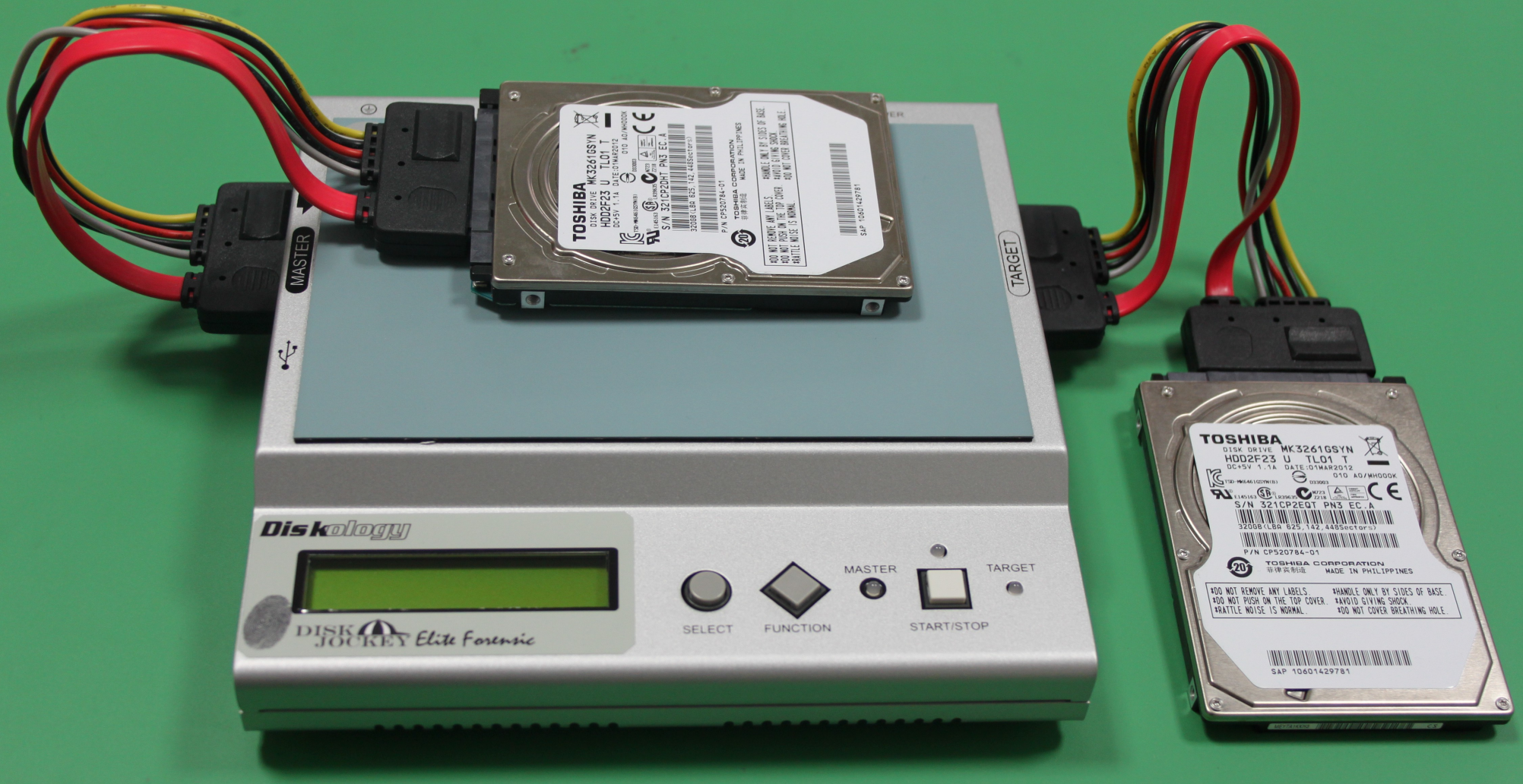
Data at Rest

Data in Use



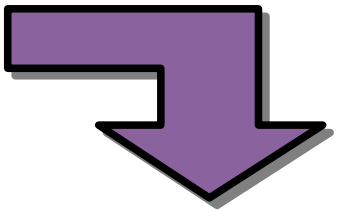
Data in Transit

Disk Forensics for ICS



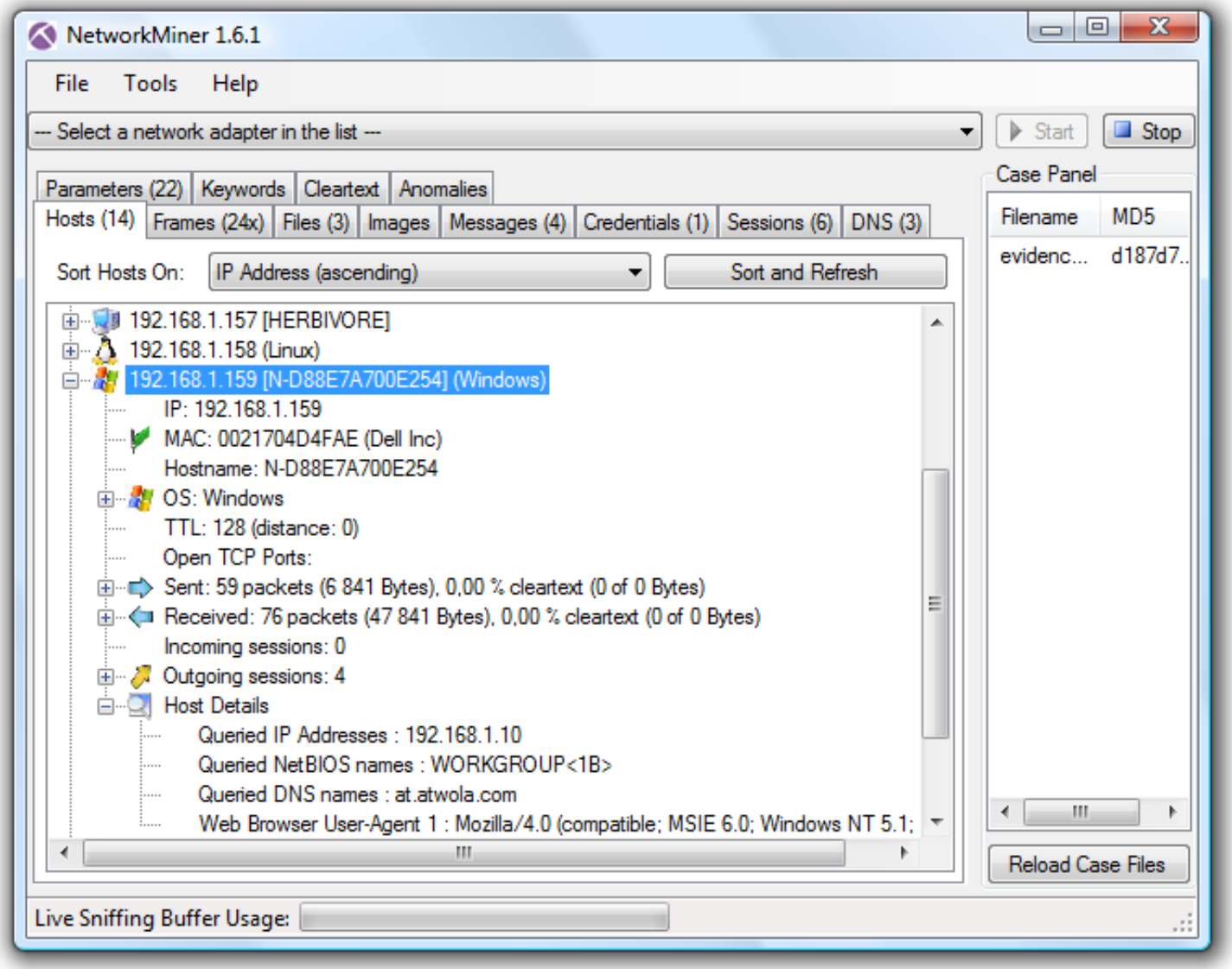
Memory Forensics

```
F:\>winpmem_1.6.0.exe ramdump.raw
Will generate a RAW image
CR3: 0x0000122000
 3 memory ranges:
Start 0x00001000 - Length 0x0009D000
Start 0x00100000 - Length 0x0
Start 0x03C00000 - Length 0x7
Acquisition mode \\.\Physical
Padding from 0x00000000 to 0x
00% 0x00001000 .
Padding from 0x0009E000 to 0x
00% 0x00100000 ..............
02% 0x03300000 ........
Padding from 0x03A04000 to 0x
92% 0x74400000 ..............
94% 0x77600000 ..............
97% 0x7A800000 ..............
99% 0x7DA00000 ....
F:\>
```

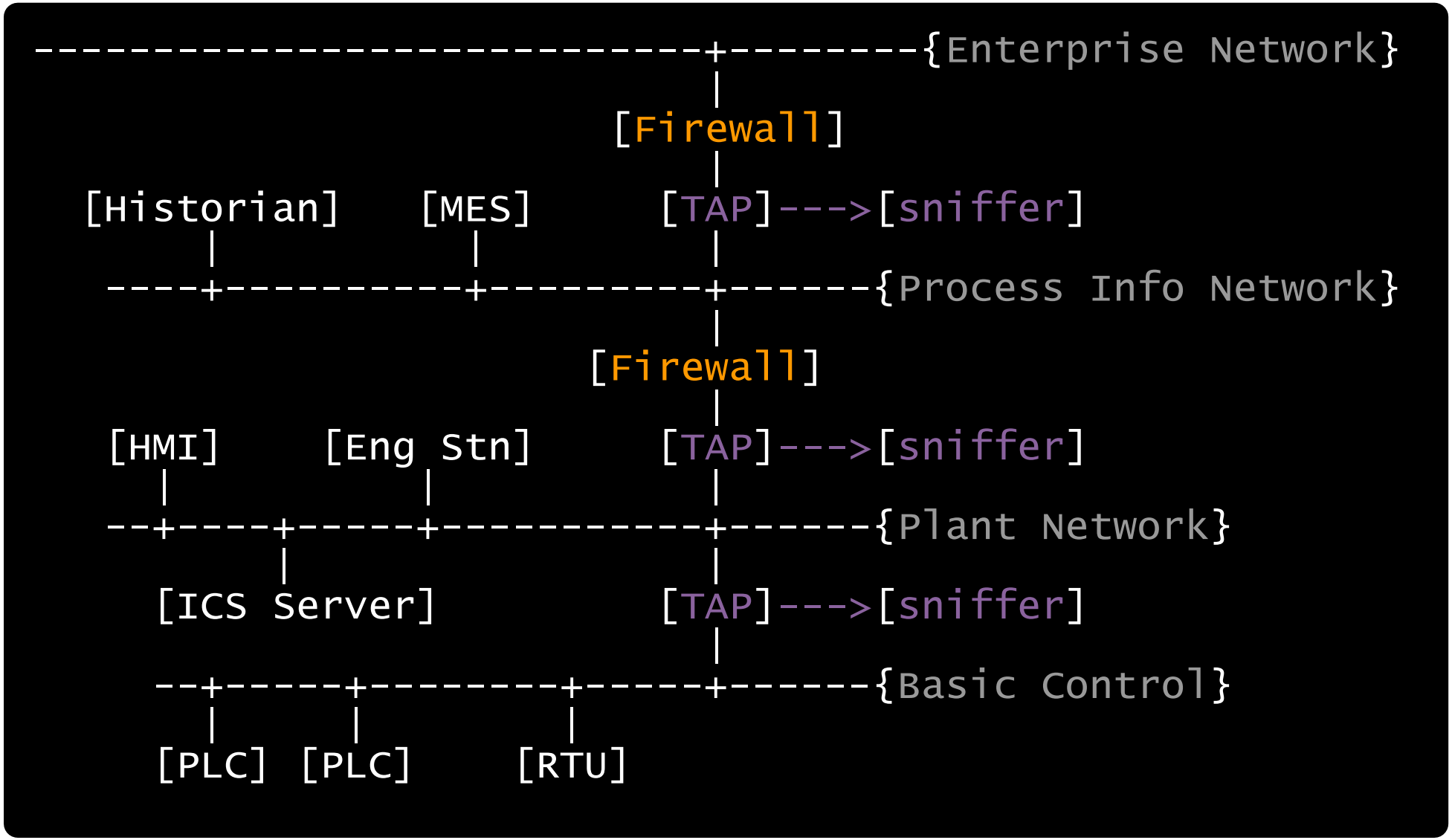


```
$ python vol.py --profile=Win7SP0x86 -f ramdump.raw pslist
Volatile Systems Volatility Framework 2.0
 Offset(V)  Name                    PID    PPID   Thds     Hnds   Time
---------- -------------------- ------ ------ ------ -------- ------------------
0x74133a30 System                    4      0     88      486 2014-10-16 15:24:58
0x752e7020 smss.exe                252      4      2       29 2014-10-16 15:24:58
0x759f3d40 csrss.exe               352    316      9      406 2014-10-16 15:25:12
0x75a5a530 wininit.exe             392    316      3       75 2014-10-16 15:25:15
0x75a5f530 csrss.exe               400    384     10      361 2014-10-16 15:25:15
0x759f5bc0 winlogon.exe            464    384      3      112 2014-10-16 15:25:18
0x75b0b318 services.exe            508    392      6      185 2014-10-16 15:25:18
0x75d393f8 lsass.exe               516    392      6      584 2014-10-16 15:25:18
0x741d1750 lsm.exe                 524    392     10      143 2014-10-16 15:25:18
0x75d5b8f8 svchost.exe             628    508      9      361 2014-10-16 15:25:19
0x750c67e0 svchost.exe             688    508      7      268 2014-10-16 15:25:20
$
```

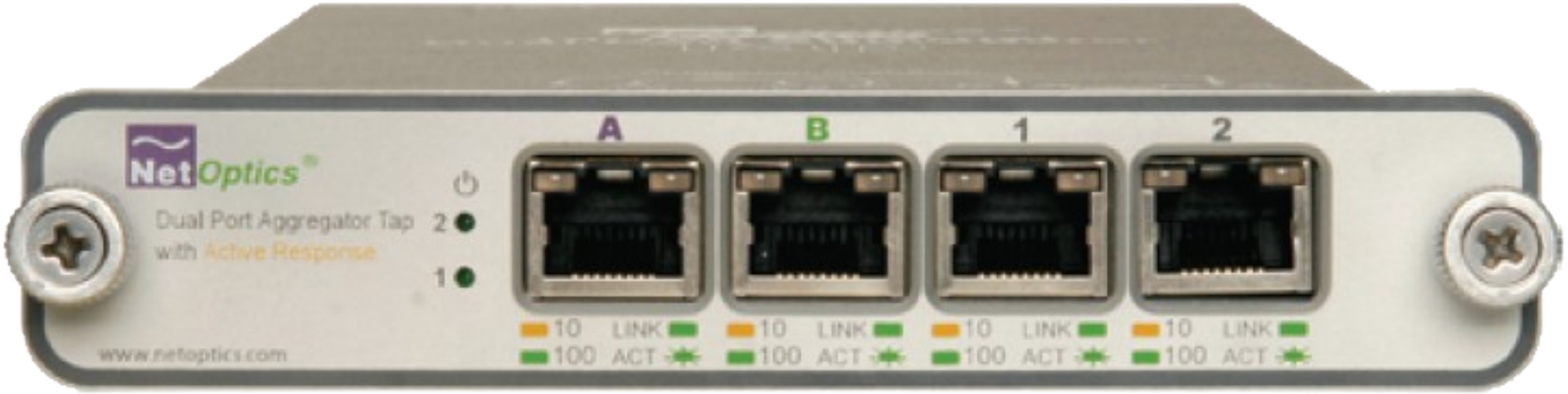
Network Forensics



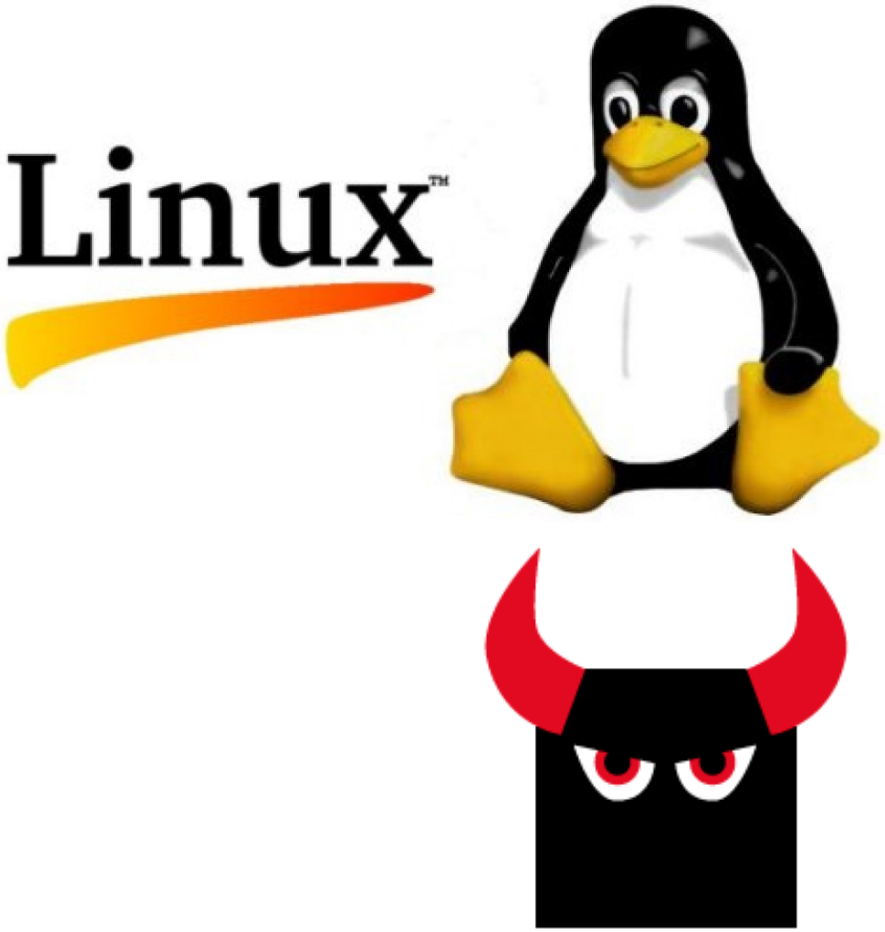
Enabling Network Forensics



Network TAP?


NetOptics
Dual Port Aggregator Tap
with Active Response
www.netoptics.com
2
1
A
B
1
2
10
100
LINK
ACT

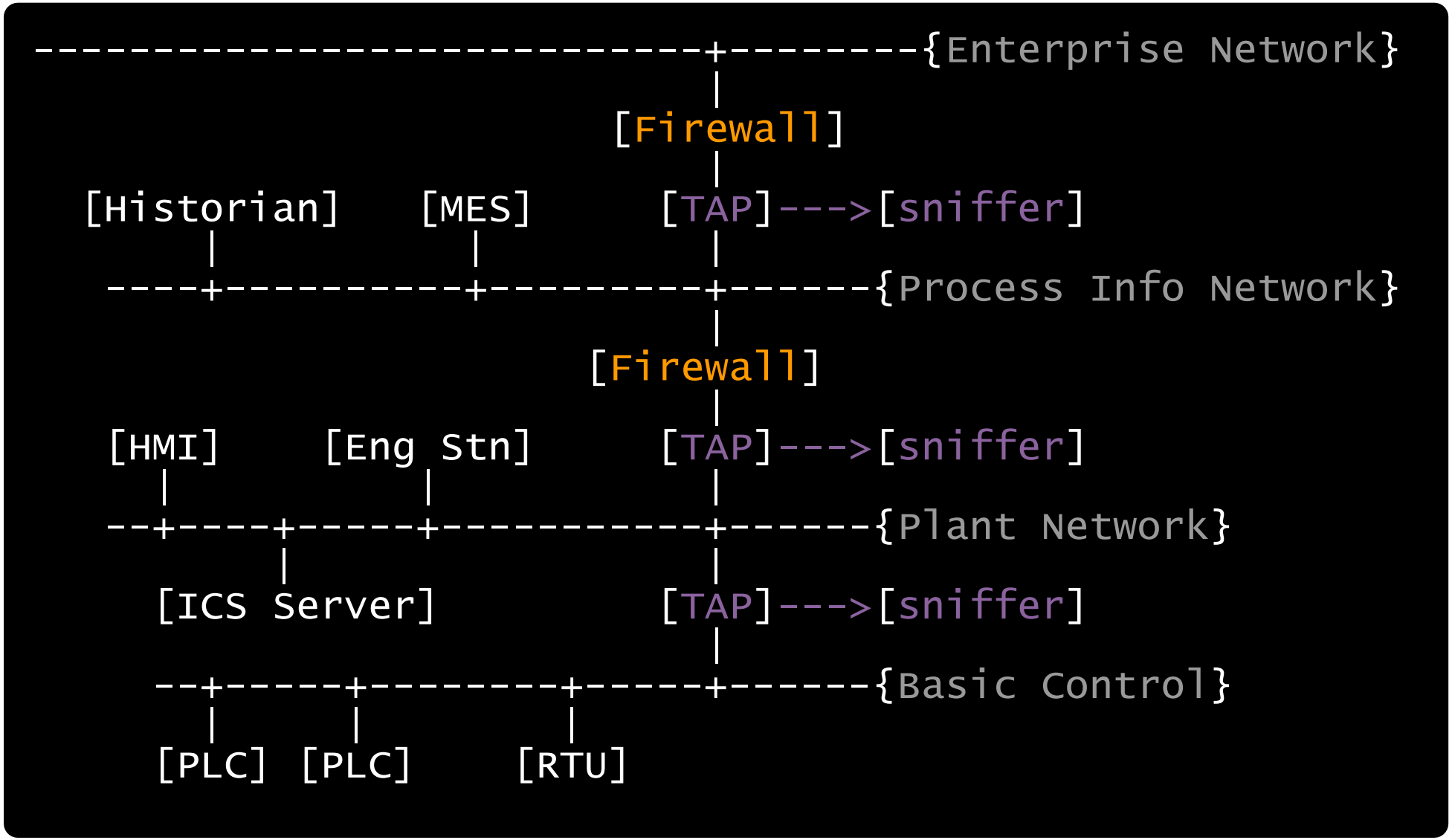
Penguin + Bull = Sniffer



netsniff-ng

the packet sniffing beast

Enabling Network Forensics



Protocol: IEC-104

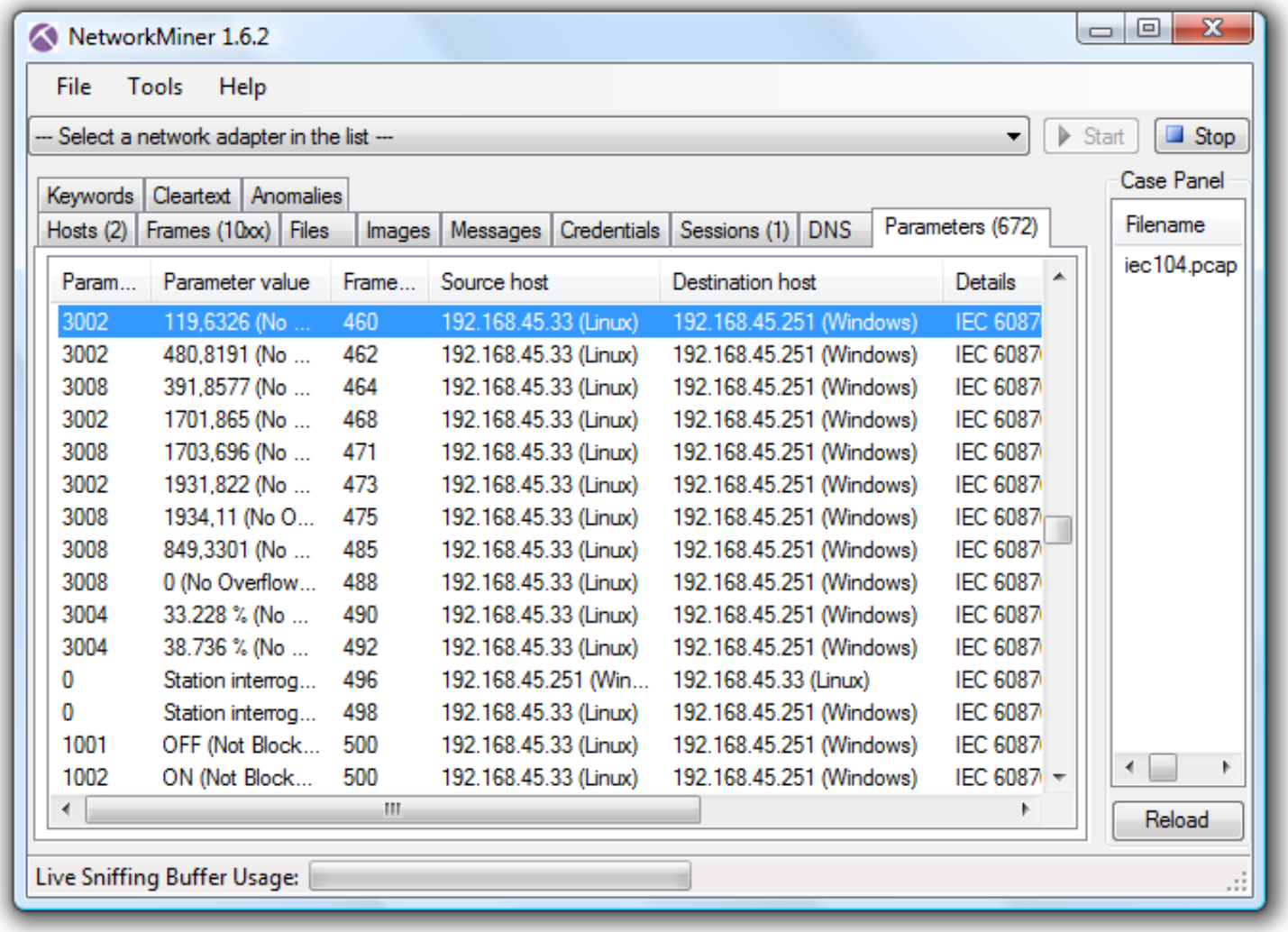
IEC 60870-5-104 (aka IEC-104)

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

IEC-104 Network Forensics

```
$ tshark -R "104asdu.float" -Eoccurrence=f -T fields -e frame.number
-e ip.src -e ip.dst -e 104asdu.causetx -e 104asdu.ioa -e 104asdu.float
-r iec104.pcap
18      192.168.45.33   192.168.45.251  20      3002    0
20      192.168.45.33   192.168.45.251  20      3005    0
30      192.168.45.33   192.168.45.251  20      3002    0
405     192.168.45.33   192.168.45.251  20      3002    0
407     192.168.45.33   192.168.45.251  20      3004    0
419     192.168.45.33   192.168.45.251  20      3002    0
421     192.168.45.33   192.168.45.251  20      3004    0
460     192.168.45.33   192.168.45.251  3       3002    119,633
462     192.168.45.33   192.168.45.251  3       3002    480,819
464     192.168.45.33   192.168.45.251  3       3008    391,858
468     192.168.45.33   192.168.45.251  3       3002    1701,86
471     192.168.45.33   192.168.45.251  3       3008    1703,7
473     192.168.45.33   192.168.45.251  3       3002    1931,82
475     192.168.45.33   192.168.45.251  3       3008    1934,11
[...]
```

IEC-104 in NetworkMiner



Protocol: OPC

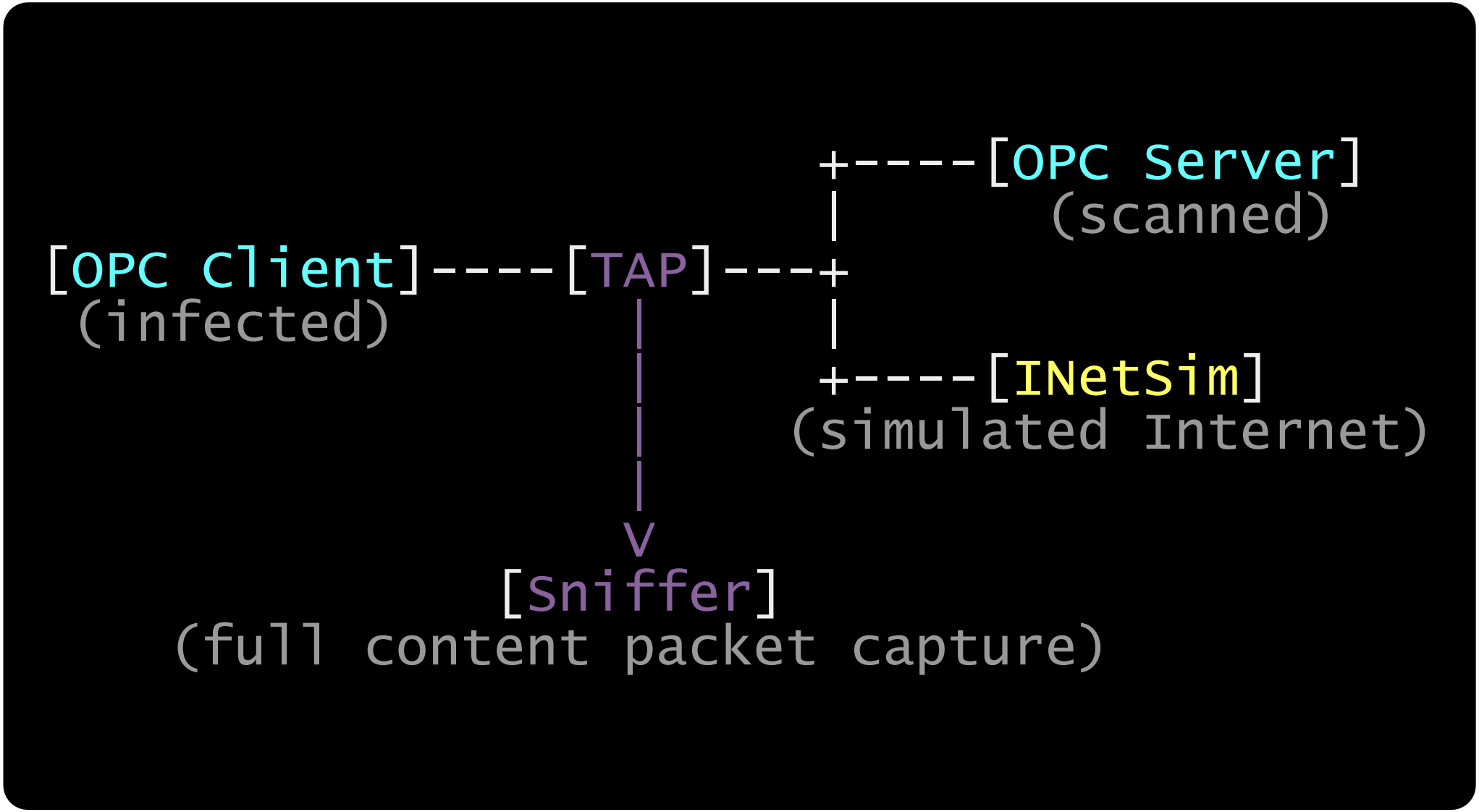
OPC = OLE for Process Control

The Hacker News™
Security in a serious way

New Variant of Havex Malware Scans for OPC Servers at SCADA Systems

Friday, July 18, 2014 Swati Khandelwal

Malware Lab Network



Havex OPC Scan

```
$ tshark -nr havex_6bfc42f7cb1364ef0bfd749776ac6d38.pcap -R dcerpc.cn_bind_to_uuid -T
fields -e ip.src -e ip.dst -e dcerpc.cn_bind_to_uuid -Eoccurrence=f -Eheader=y
ip.src              ip.dst              dcerpc.cn_bind_to_uuid
192.168.0.111   192.168.0.112   000001a0-0000-0000-c000-000000000046
192.168.0.111   192.168.0.112   9dd0b56c-ad9e-43ee-8305-487f3188bf7a <- OPC Server List 2
192.168.0.111   192.168.0.112   55c382c8-21c7-4e88-96c1-becfb1e3f483 <- OPC Enum GUID
192.168.0.111   192.168.0.112   00000143-0000-0000-c000-000000000046
192.168.0.111   192.168.0.112   00000143-0000-0000-c000-000000000046
192.168.0.111   192.168.0.112   39c13a4d-011e-11d0-9675-0020afd8adb3 <- OPC Server
192.168.0.111   192.168.0.112   39227004-a18f-4b57-8b0a-5235670f4468 <- OPC Browse
$
```

Havex C&C Traffic

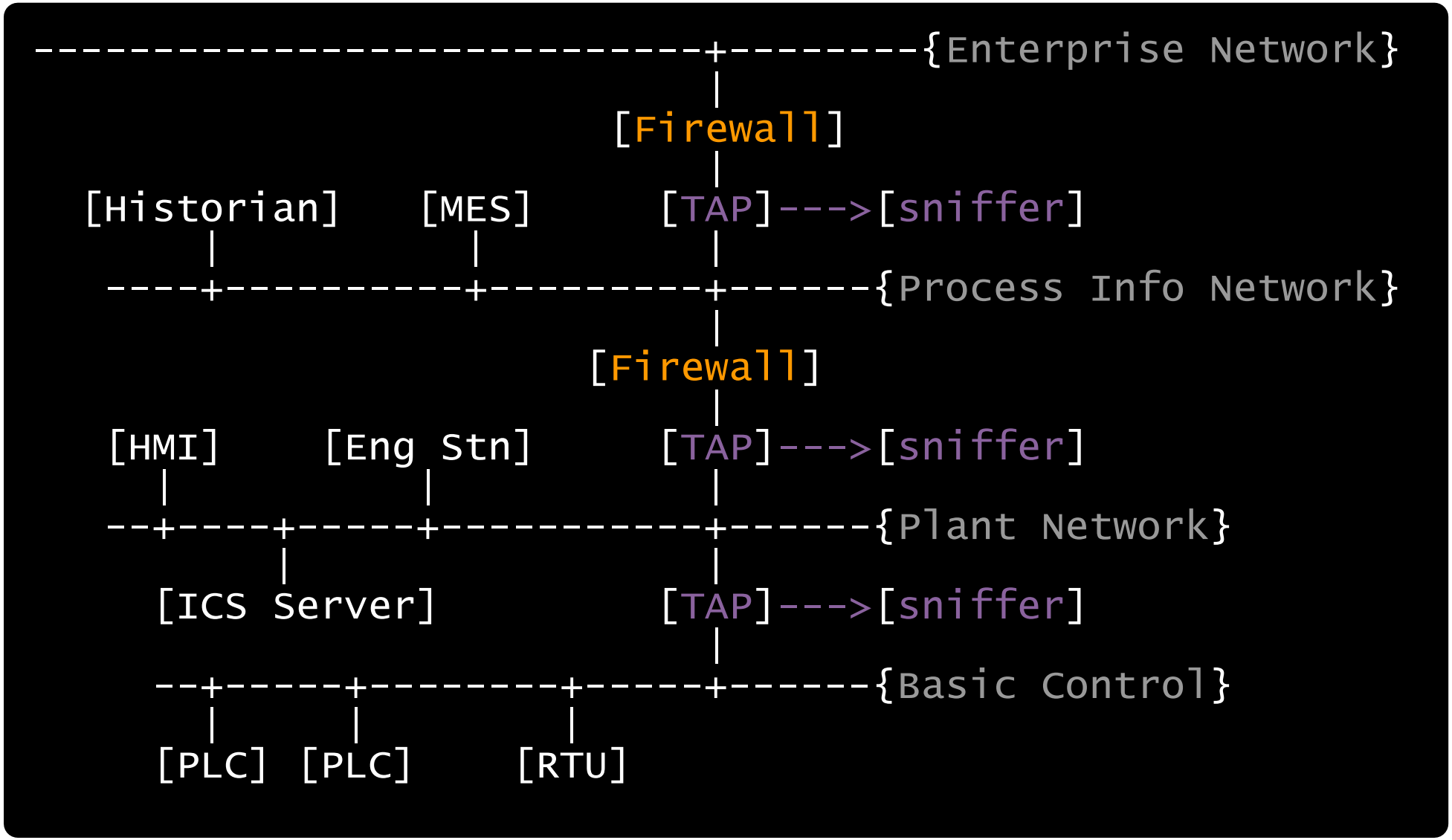
```
$ tshark -nr havex_0a9ae7fdcd9a9fe0d8c5c106e8940701.pcap
-R http.request -T fields -e ip.src -e http.host -e
http.request.method -e http.request.uri
192.168.0.111  rapidecharge.gigfa.com  POST
/blogs/wp-content/plugins/buddypress/bp-settings/bp-
settings-src.php?id=8465119383478719609009 8FD80-
c8a7af419640516616c342b13efab
&v1=043&v2=170393861&q=45474bca5c3a10c8e94e56543c2bd
$
```

Havex IDS Signature

Emerging Threats IDS signature 2018251:

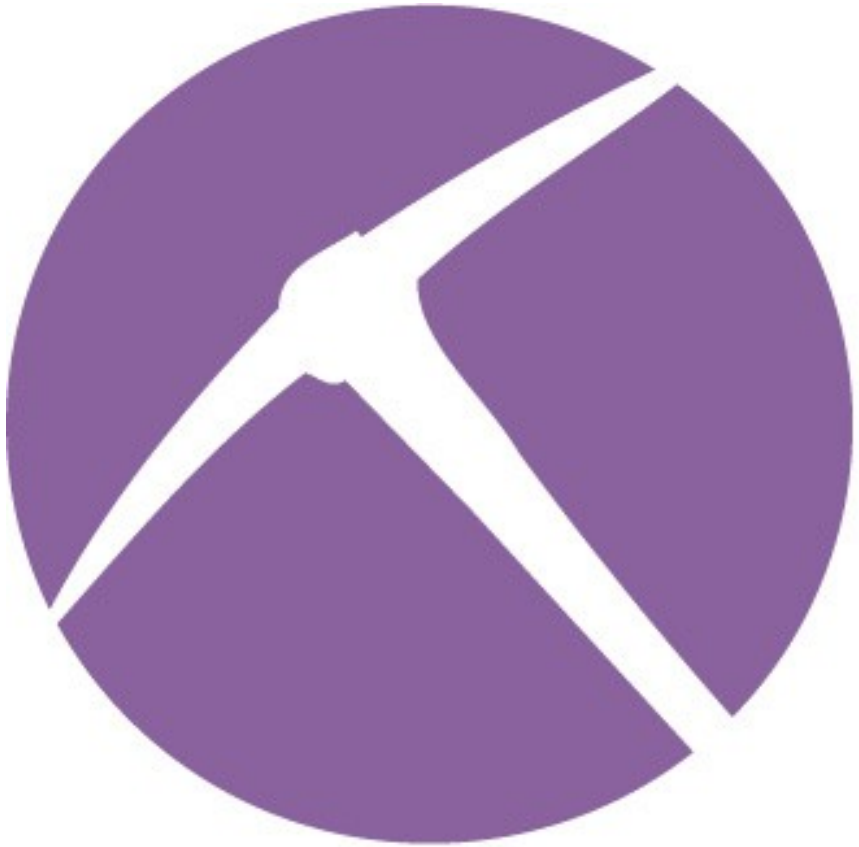

```
#alert tcp $HOME_NET any -> $EXTERNAL_NET
$HTTP_PORTS (msg:"ET DELETED Havex Rat Check-in
URI Struct"; flow:established,to_server;
content:"POST"; http_method; content:!"Referer|3a
20|"; content:".php?id"; http_uri;
content:"&v1="; http_uri; content:"&v2=";
http_uri; content:"&q="; http_uri; pcre:"/\.php\?
id=[A-F0-9]+\-[A-F0-9]+&v1=[A-F0-9]+&v2=[A-F0-
9]+&q=[A-F0-9]+$/U";
reference:md5,6557d6518c3f6bcb8b1b2de77165c962;
classtype:trojan-activity; sid:2018251; rev:1;)
```

Enabling Network Forensics



More ICS in NetworkMiner

DNP3
ICCP
IEC 61850
Modbus/TCP
OPC
Profinet
Siemens S7
etc...



CONTACT INFO

E-mail: erik.hjelmvik [at] netresec.com
Twitter: @netresec