# Tux's Angels:
# Incident Response Unravelled

linux.conf.au MEL8OURNE2008

# Tux's Angels: Incident Response Unravelled

- Something to lighten the mood...

# When Incident Response goes BAD.

Please. Think of the kittens.

# Who we are

- Amelia, Kate, Vanessa
  - IT Security Geeks
  - Department of Defence
  - Information Security Group
  - Computer Network Vulnerability Team (CNVT)

# What we do

- For Federal and State Government:
  - 24/7 Incident response
  - IT Security advice and assistance
  - Vulnerability assessments
  - Penetration testing / red teaming
  - Research and Development
  - Education and Training

# Agenda

- Incident response
- Linux + FOSS
- Investigation
- Conclusion

# Agenda

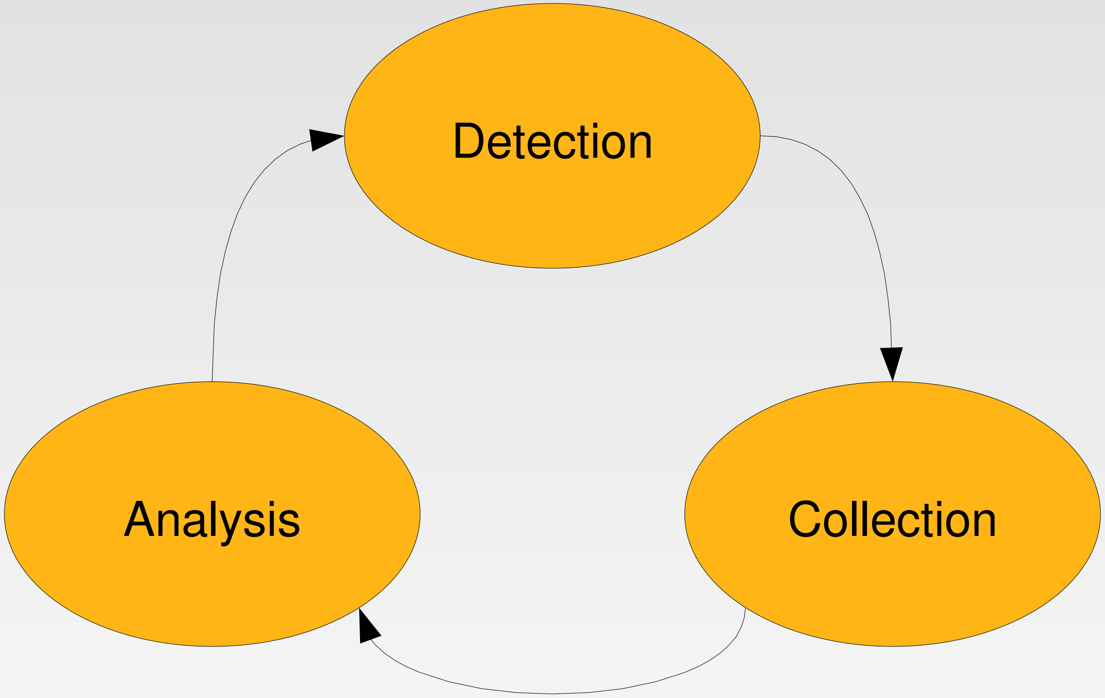
- **Incident response**
- Linux + FOSS
- Investigation
- Conclusion

# Incident response

- Incident: Events that threaten IT Security
- Incident response: Process of handling this situation
- Things to keep in mind:
  - Inform management
  - Involve law enforcement for criminal activity
  - Preserve forensic integrity

# Incident response

- IR life cycle:
  - Detection
  - Collection
  - Analysis



# Agenda

- **Incident response**
- Linux + FOSS
- Investigation
- Conclusion

# Agenda

- Incident response
- **Linux + FOSS**
- Investigation
- Conclusion

# Linux + FOSS: why?

- Why do we use Linux in Incident Response?
  - Not invasive
  - Multiple filesystem support
  - More OS control
  - Loopback device
- Why FOSS?
  - Cutting edge technology
  - Customisable, and more control
- Free!

# Linux + FOSS: tool selection

- How do we select tools for IR?
  - Ease of installation
  - Easy to understand, use and configure
  - How accurate and updated it is
  - Support and documentation available
  - Reputation of the developers

# Agenda

- Incident response
- **Linux + FOSS**
- Investigation
- Conclusion

# Agenda

- Incident response
- Linux + FOSS
- **Investigation**
- Conclusion

# Investigation

- The incident
- IR life cycle
    - Detection
    - Collection
    - Analysis

# Investigation

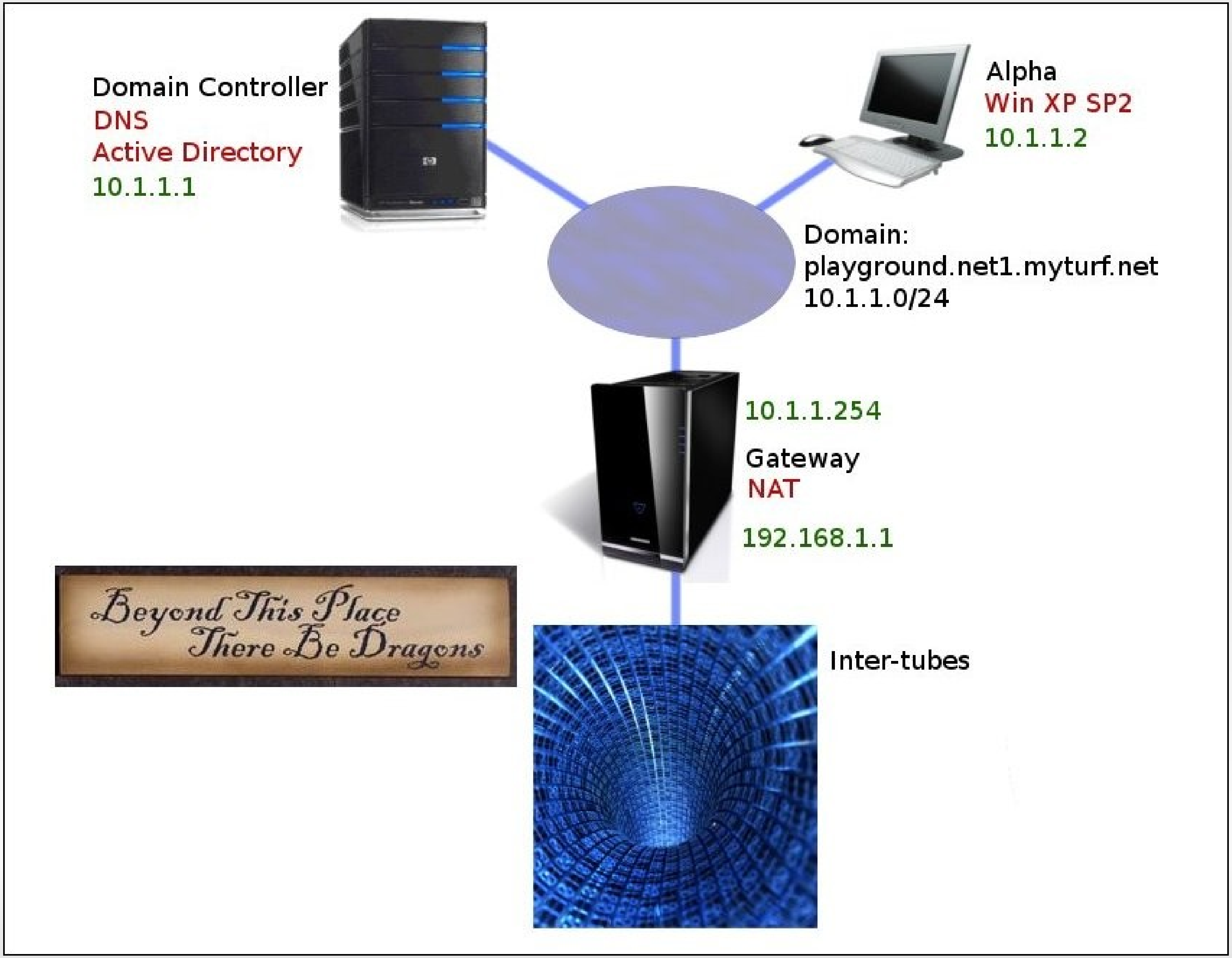
- **The incident**
- IR life cycle
  - Detection
  - Collection
  - Analysis

# The incident

- **Who?** Administrator from Playground Inc.
- **What?** Suspected compromise of workstation ”ALPHA”
- **When?** Reported at 4:30pm on 19th Dec 2007
- playground.net1.myturf.net domain
- Requested on-site assistance from Tux's Angels

# The network

# The network



Domain Controller
DNS
Active Directory
10.1.1.1

Alpha
Win XP SP2
10.1.1.2

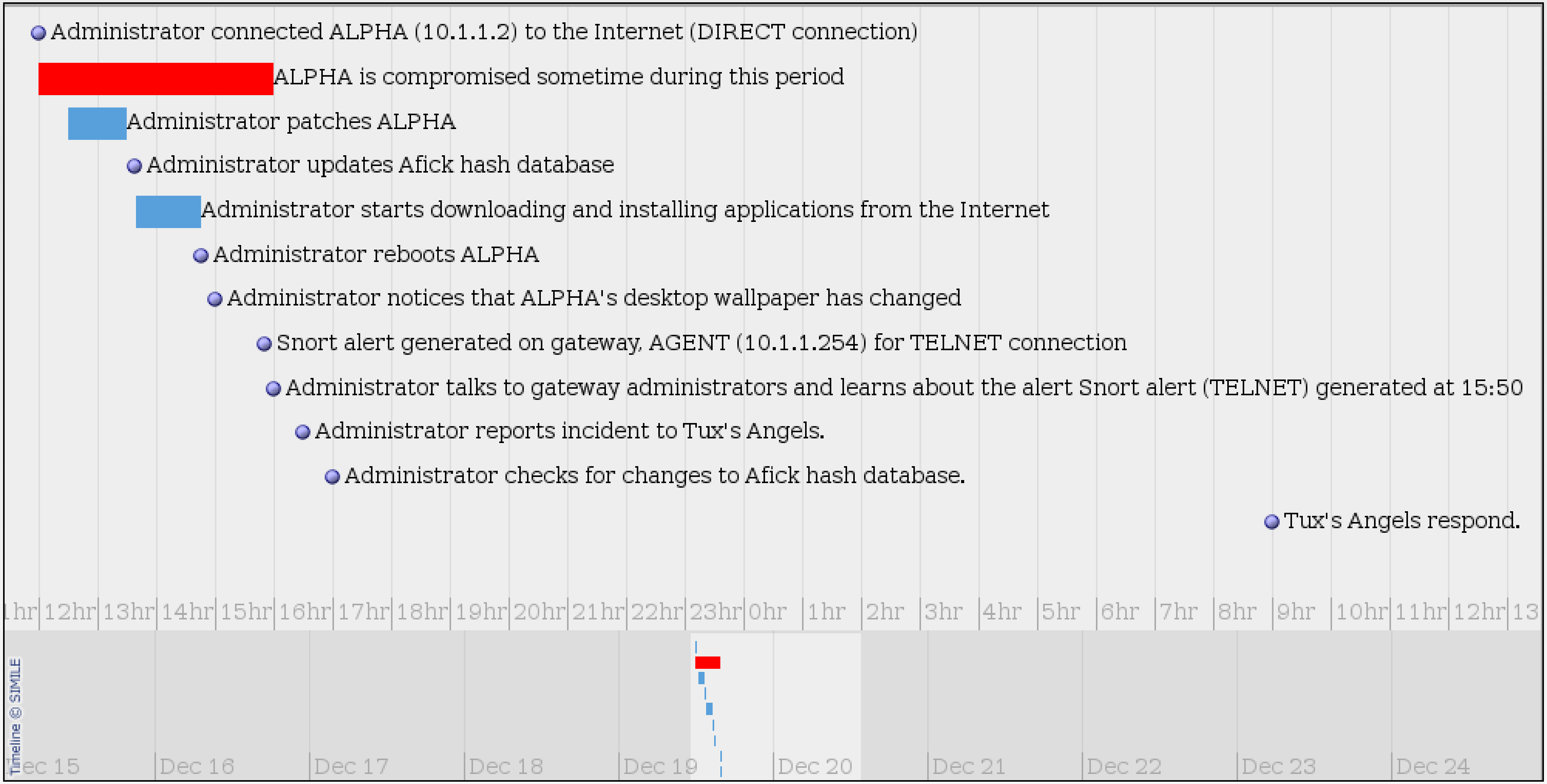
Domain:
playground.net1.myturf.net
10.1.1.0/24

10.1.1.254
Gateway
NAT
192.168.1.1

Inter-tubes

# Timeline: what we know

# Timeline: what we know



Administrator connected ALPHA (10.1.1.2) to the Internet (DIRECT connection)

ALPHA is compromised sometime during this period

Administrator patches ALPHA

Administrator updates Afick hash database

Administrator starts downloading and installing applications from the Internet

Administrator reboots ALPHA

Administrator notices that ALPHA's desktop wallpaper has changed

Snort alert generated on gateway, AGENT (10.1.1.254) for TELNET connection

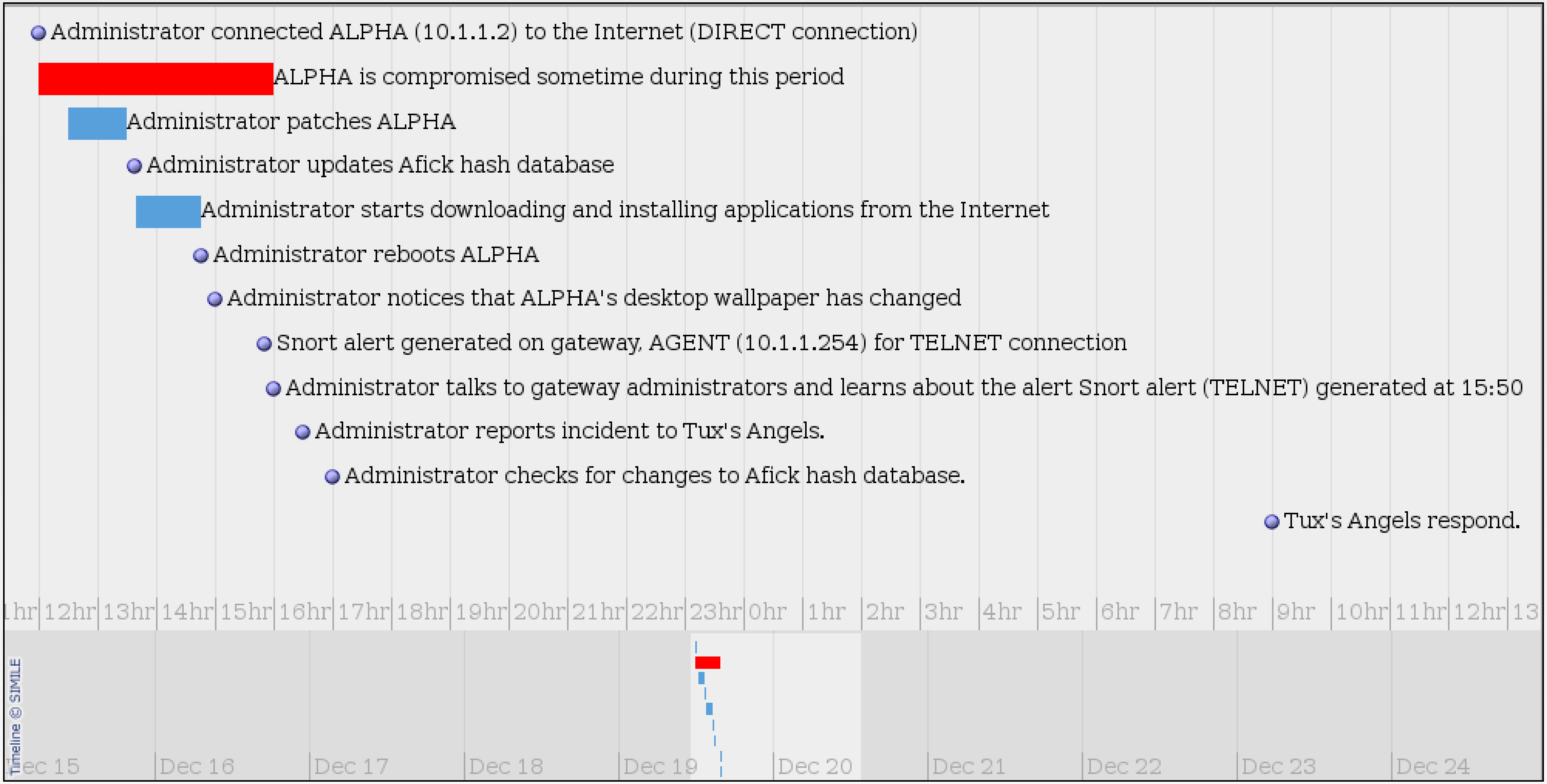
Administrator talks to gateway administrators and learns about the alert Snort alert (TELNET) generated at 15:50

Administrator reports incident to Tux's Angels.

Administrator checks for changes to Afick hash database.

Tux's Angels respond.

# Timeline: what we know



Administrator connected ALPHA (10.1.1.2) to the Internet (DIRECT connection)

ALPHA is compromised sometime during this period

Administrator patches ALPHA

Administrator updates Afick hash database

Administrator starts downloading and installing applications from the Internet

Administrator reboots ALPHA

Administrator notices that ALPHA's desktop wallpaper has changed

Snort alert generated on gateway, AGENT (10.1.1.254) for TELNET connection

Administrator talks to gateway administrators and learns about the alert Snort alert (TELNET) generated at 15:50

Administrator reports incident to Tux's Angels.

Administrator checks for changes to Afick hash database.

Tux's Angels respond.

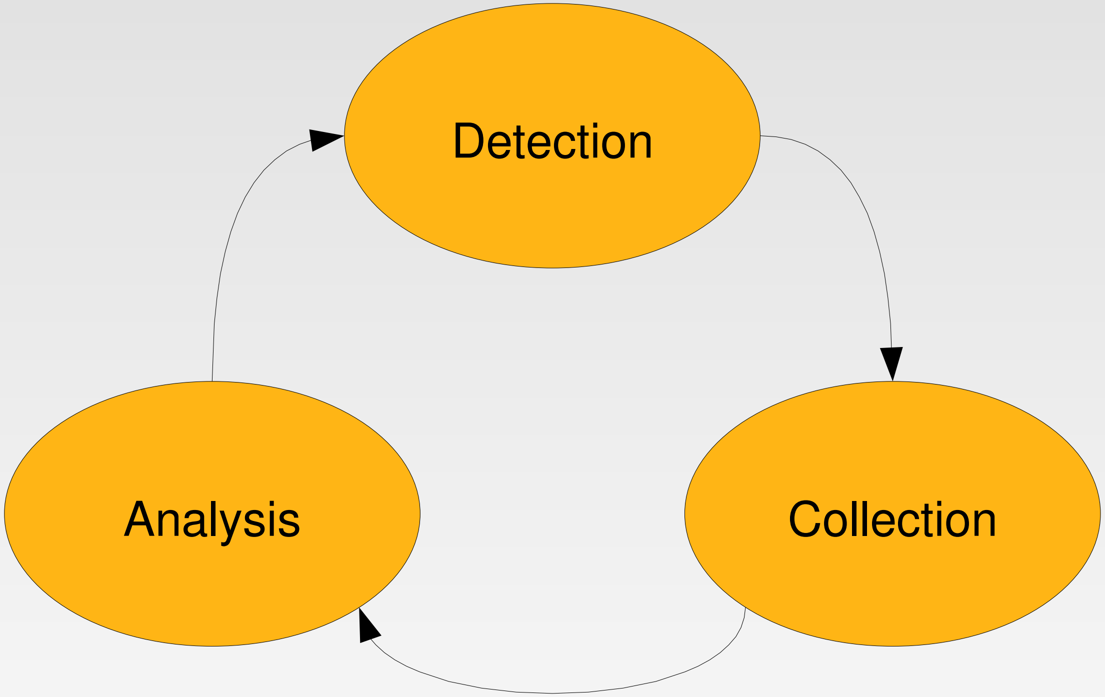
Simile Timeline: http://simile.mit.edu/timeline/

# Investigation

- **The incident**
- IR life cycle
  - Detection
  - Collection
  - Analysis

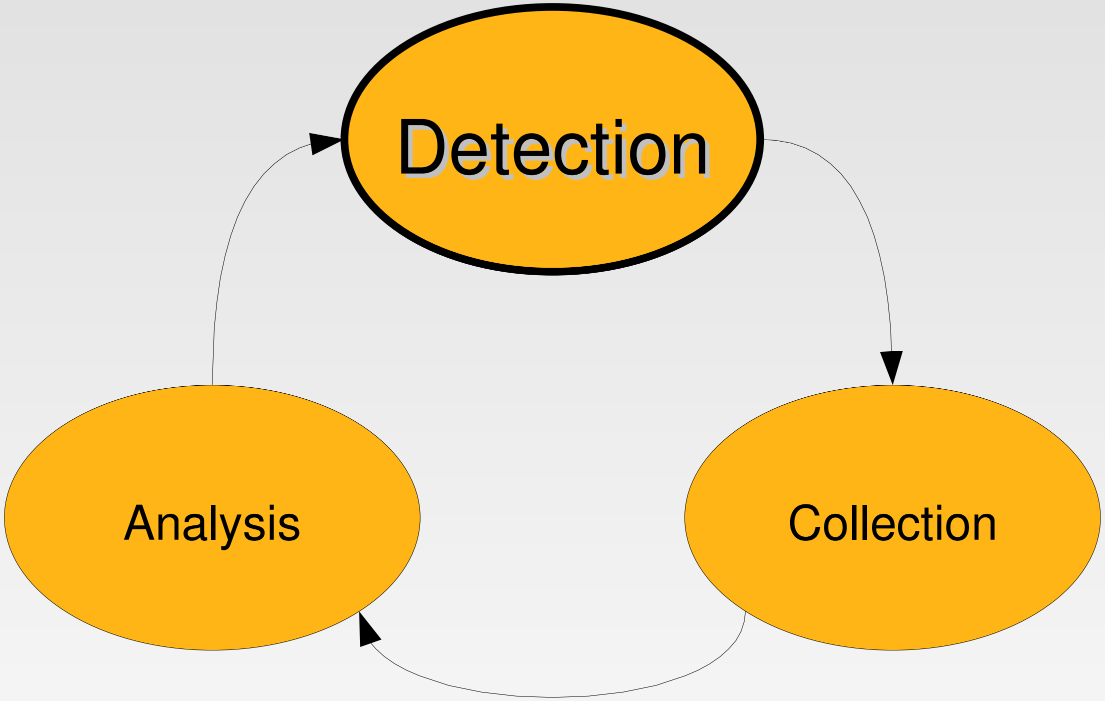
# Investigation

- The incident
- **IR life cycle**
  - Detection
  - Collection
  - Analysis



# Investigation

- The incident
- **IR life cycle**
  - **Detection**
  - Collection
  - Analysis



# Detection

- Finding out if a security incident occurred
- May come from a variety of sources:
  - IDS
  - Logs
  - Users
  - Odd system behaviour
- Use all tools and resources available

# Detection

- Variety of tools can be used to detect a security incident
- These can be broken down into:
  - Network-Based Intrusion Detection Systems (NIDS)
  - Host-Based Intrusion Detection Systems (HIDS)
  - Log watch and alerting tools

# Detection: NIDS

- Network-based Intrusion Detection System
- NIDS tools they considered using
    - Squil
    - EasyIDS
- Their NIDS tool of choice
    - Snort with BASE

# Detection: HIDS

- Host-based Intrusion Detection System
- HIDS tools they considered using
  - AIDE
  - Labrador
- Their HIDS tool of choice
  - Afick

# Detection: Log watch and alerting

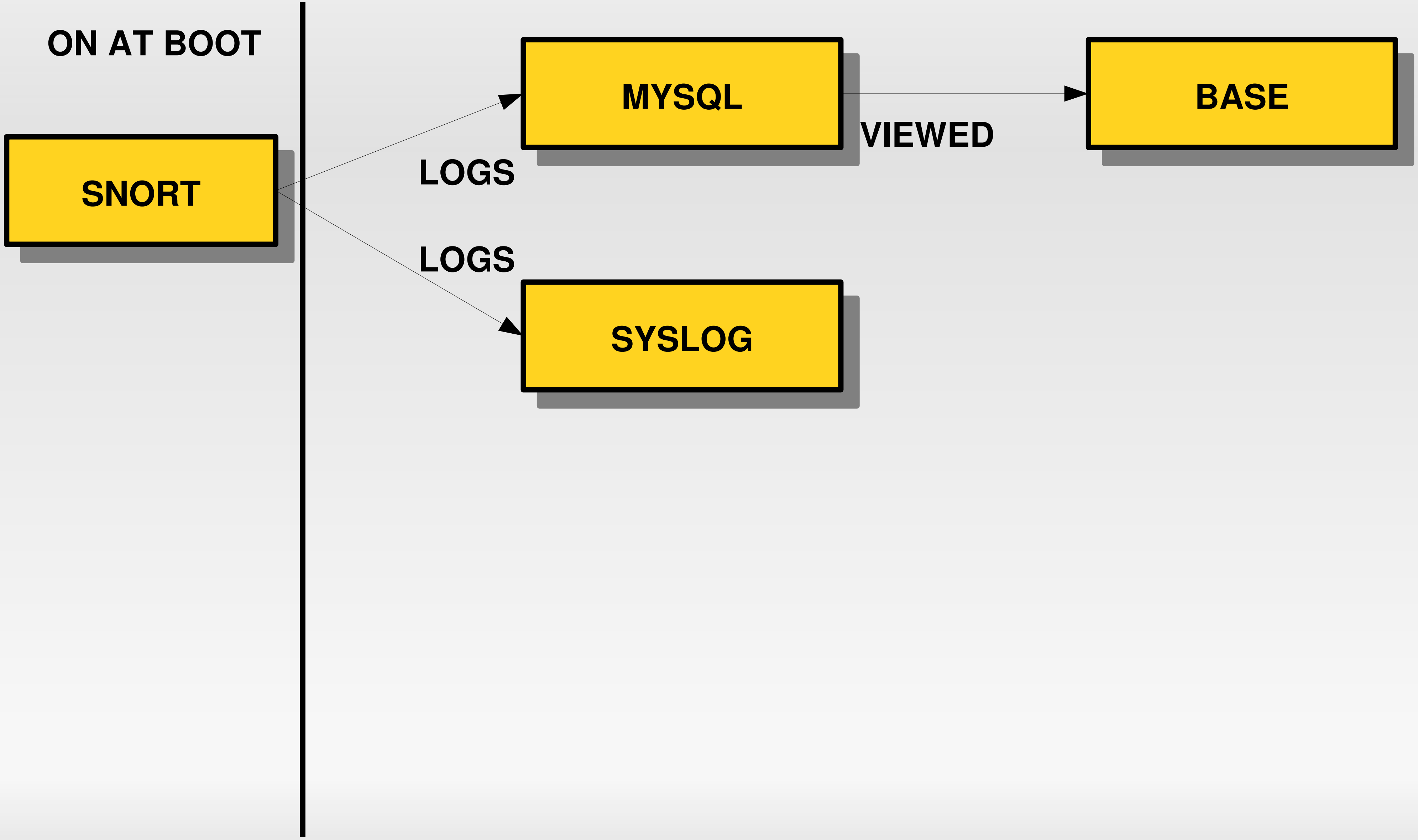
- Log watch and alerting
- Logging and alerting tools they considered using
  - LogCheck
  - Devialog
- Their logging and alerting tool of choice
  - Swatch

# Detection: Custom IDS Solution

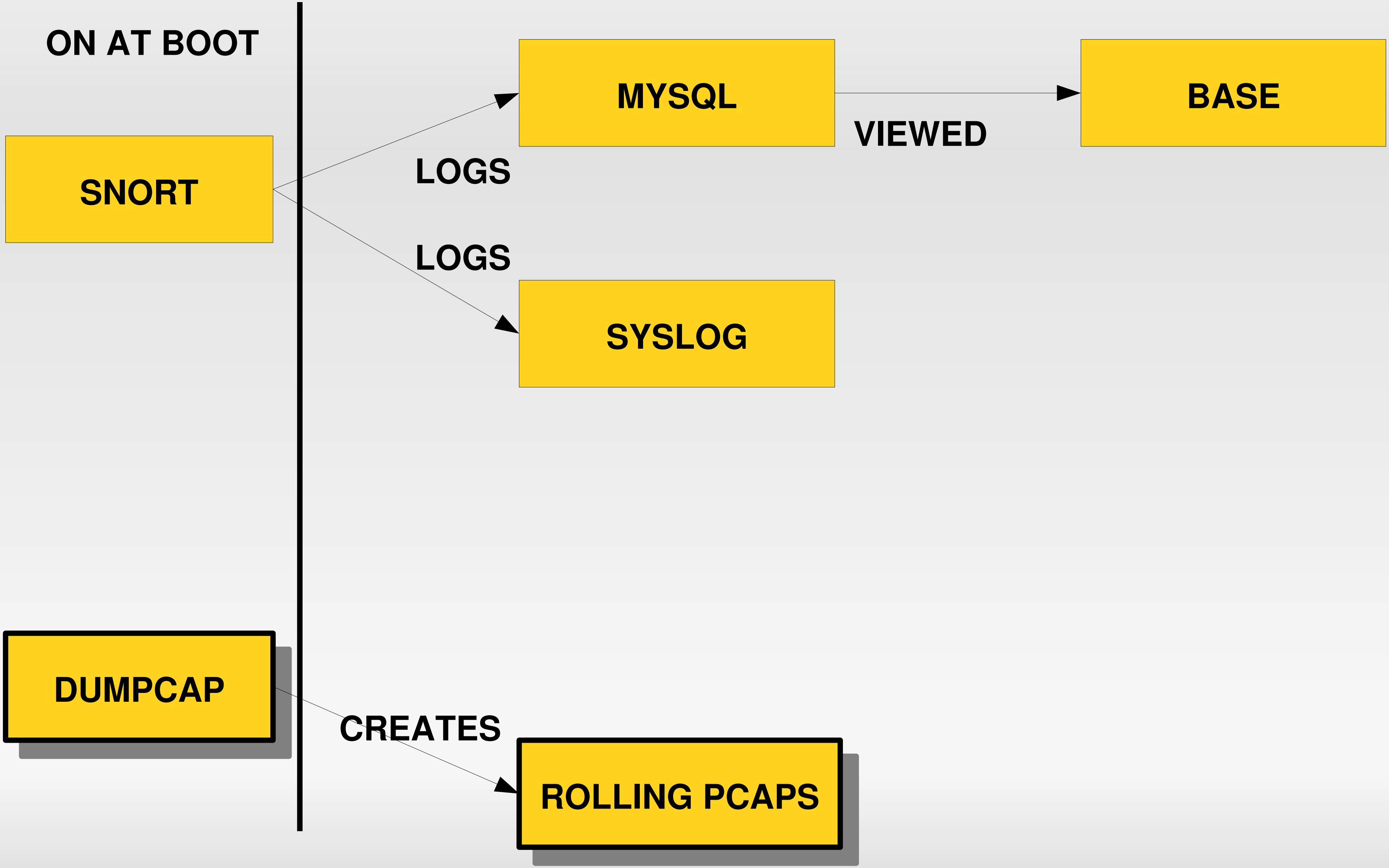
- Their custom IDS solution!

# Detection: Custom IDS Solution

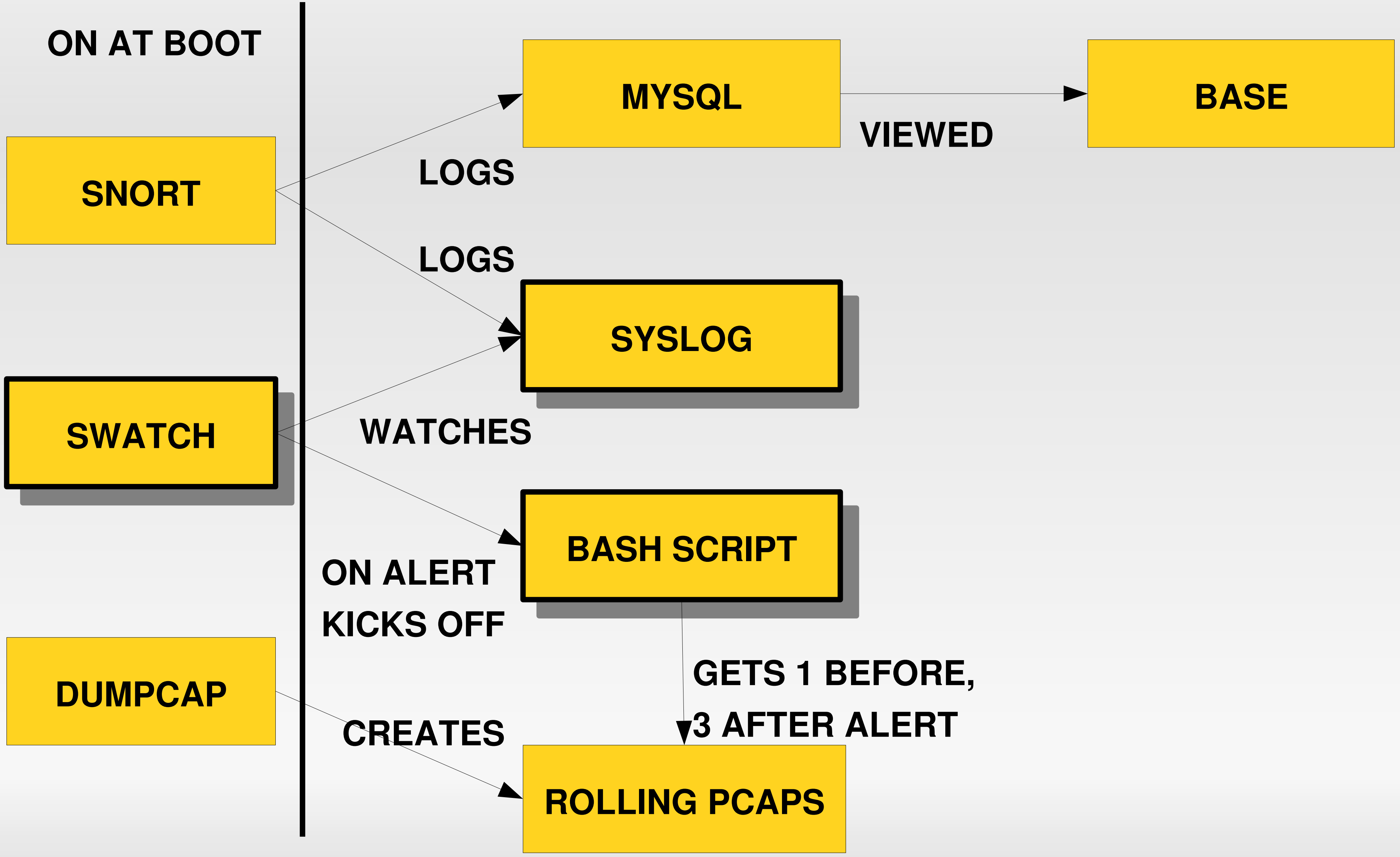
# Detection: Custom IDS Solution



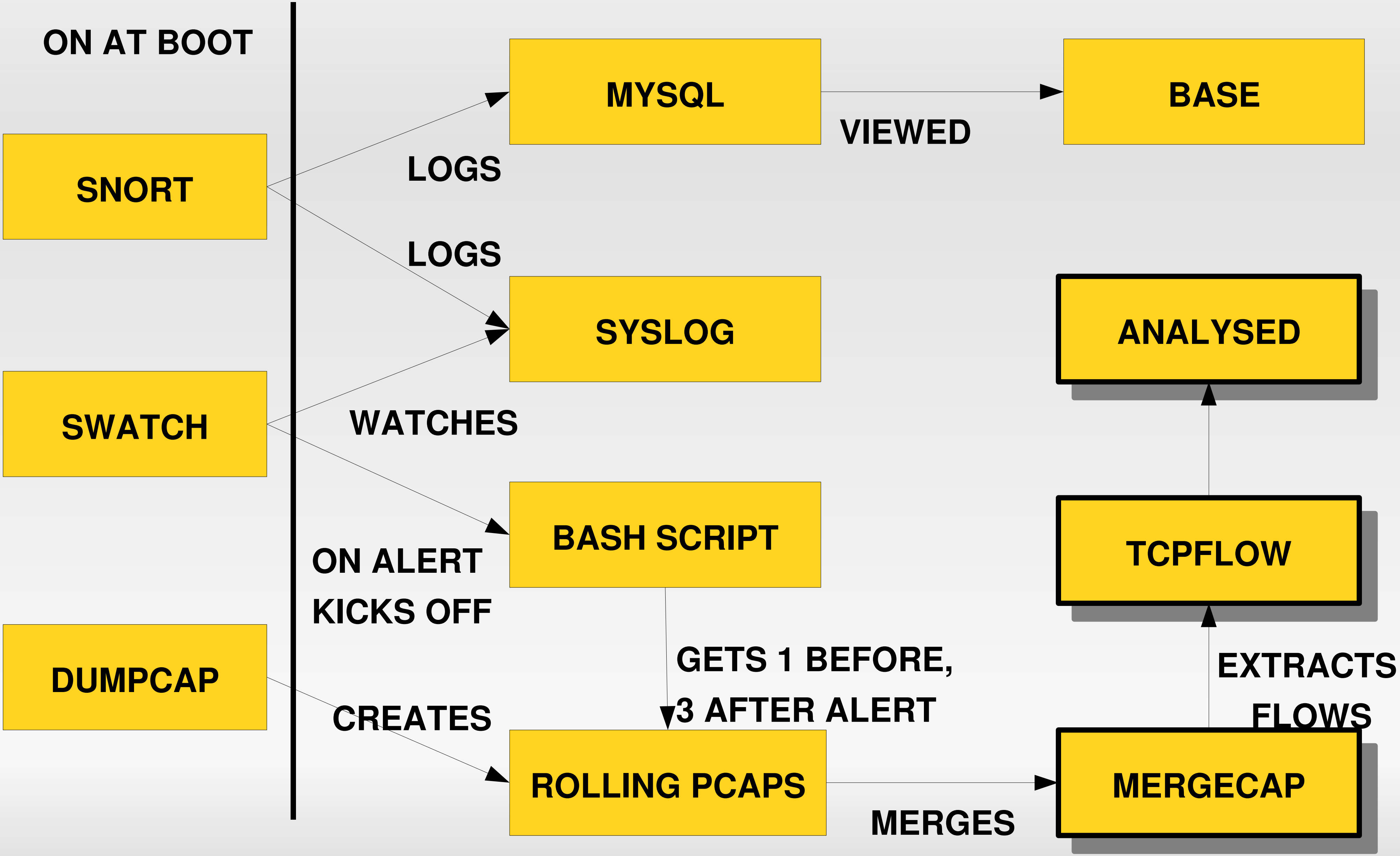
# Detection: Custom IDS Solution



# Detection: Custom IDS Solution



# Detection: Custom IDS Solution



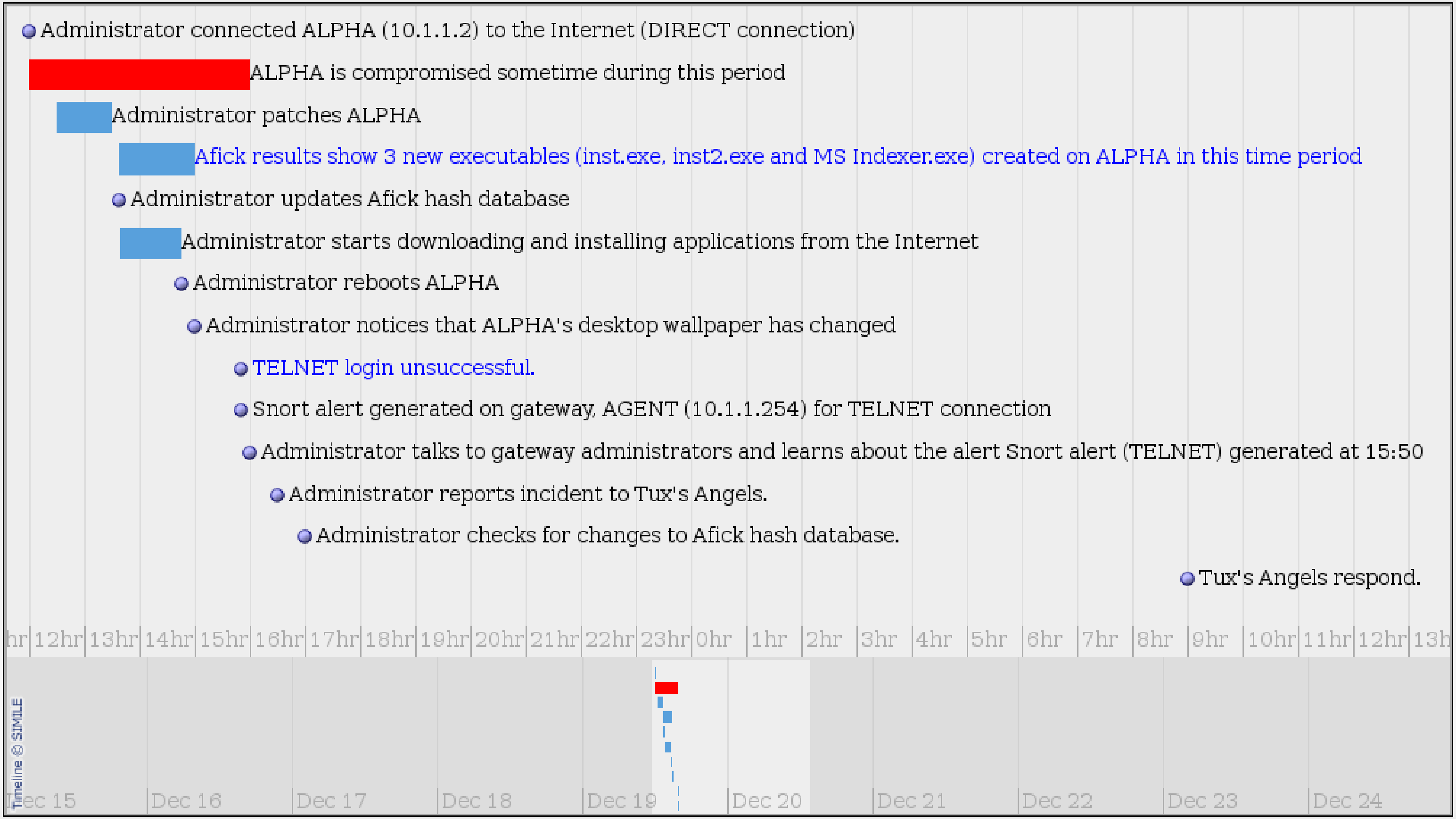
# DEMO:

## Detecting an incident using snort, swatch, tcpflow and BASE

# Detection: results

- Suspect compromise: YES
- Snort – unsuccessful TELNET login from ALPHA to Internet box
- Afick – 3 new unexplained exe's:
  - inst.exe
  - inst2.exe
  - MS Indexer.exe
- Information passed to Tux's Angels

# Timeline + Detection: what we know



Administrator connected ALPHA (10.1.1.2) to the Internet (DIRECT connection)

ALPHA is compromised sometime during this period

Administrator patches ALPHA

Afick results show 3 new executables (inst.exe, inst2.exe and MS Indexer.exe) created on ALPHA in this time period

Administrator updates Afick hash database

Administrator starts downloading and installing applications from the Internet

Administrator reboots ALPHA

Administrator notices that ALPHA's desktop wallpaper has changed

TELNET login unsuccessful.

Snort alert generated on gateway, AGENT (10.1.1.254) for TELNET connection

Administrator talks to gateway administrators and learns about the alert Snort alert (TELNET) generated at 15:50

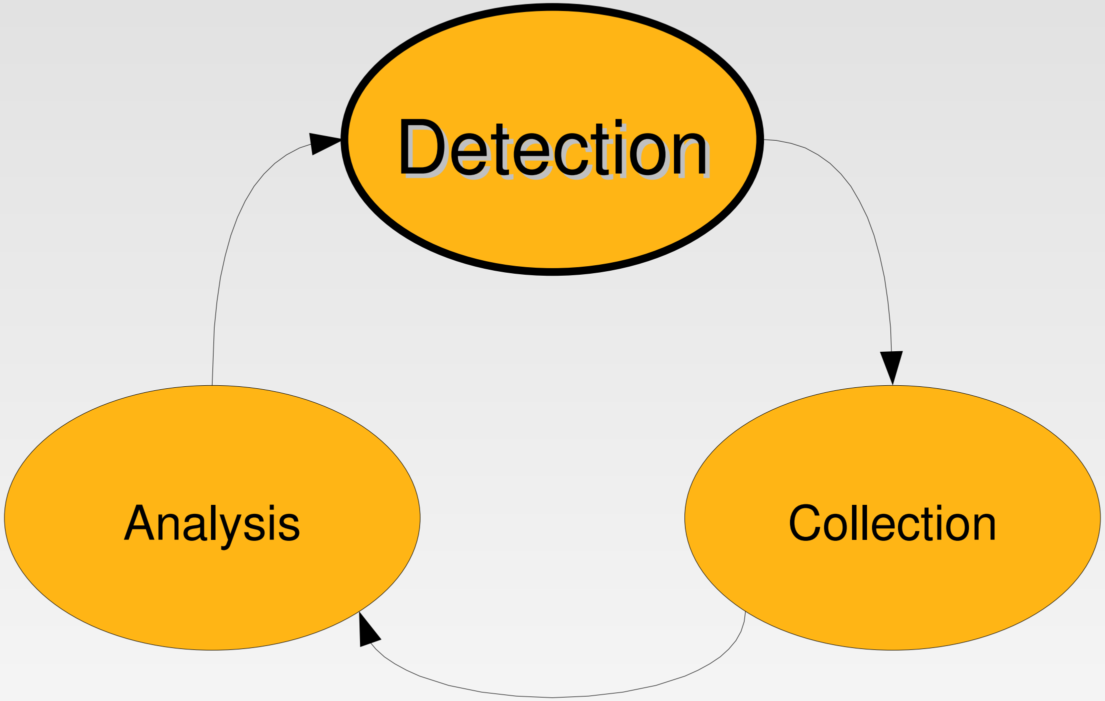
Administrator reports incident to Tux's Angels.

Administrator checks for changes to Afick hash database.

Tux's Angels respond.

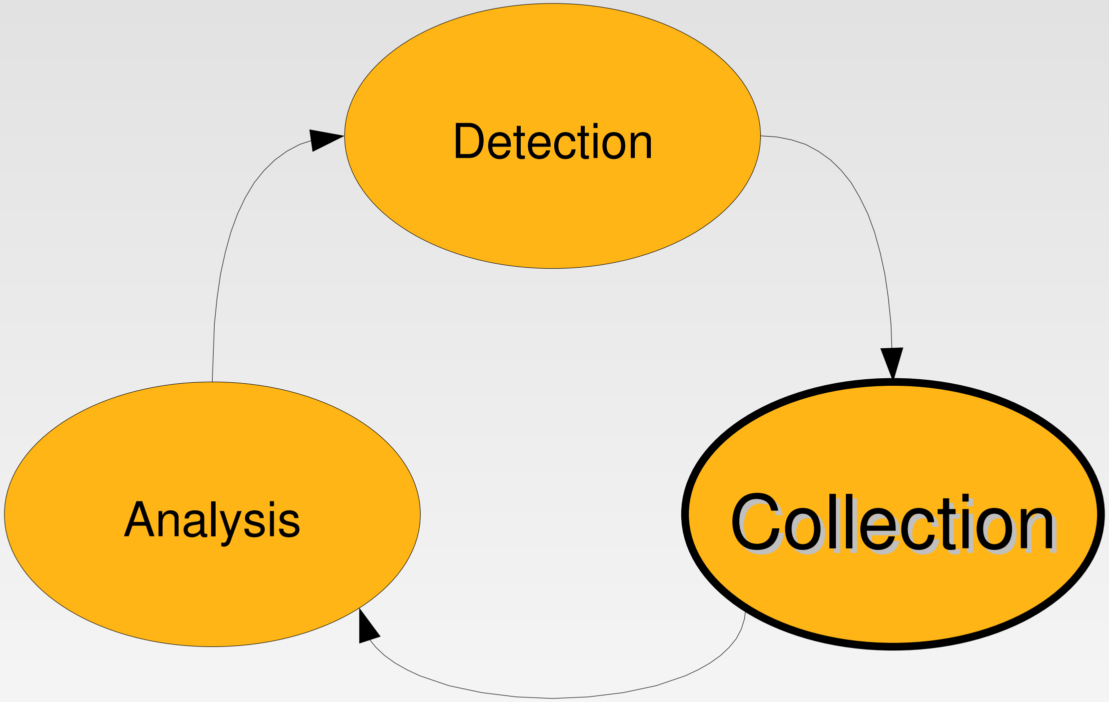
# Investigation

- The incident
- **IR life cycle**
  - **Detection**
  - Collection
  - Analysis



# Investigation

- The incident
- **IR life cycle**
  - Detection
  - **Collection**
  - Analysis



# Collection

- Acquiring data to determine occurrences related to a specific event
  - Collect data
  - Verify data

# Collection

- Data can come from a variety of sources:
  - network
  - memory
  - disk

# Collection: network

- Collecting network data
- Tools we considered using:
  - dumpcap
  - Wireshark
- Tool of choice:
  - tcpdump

# Collection: memory

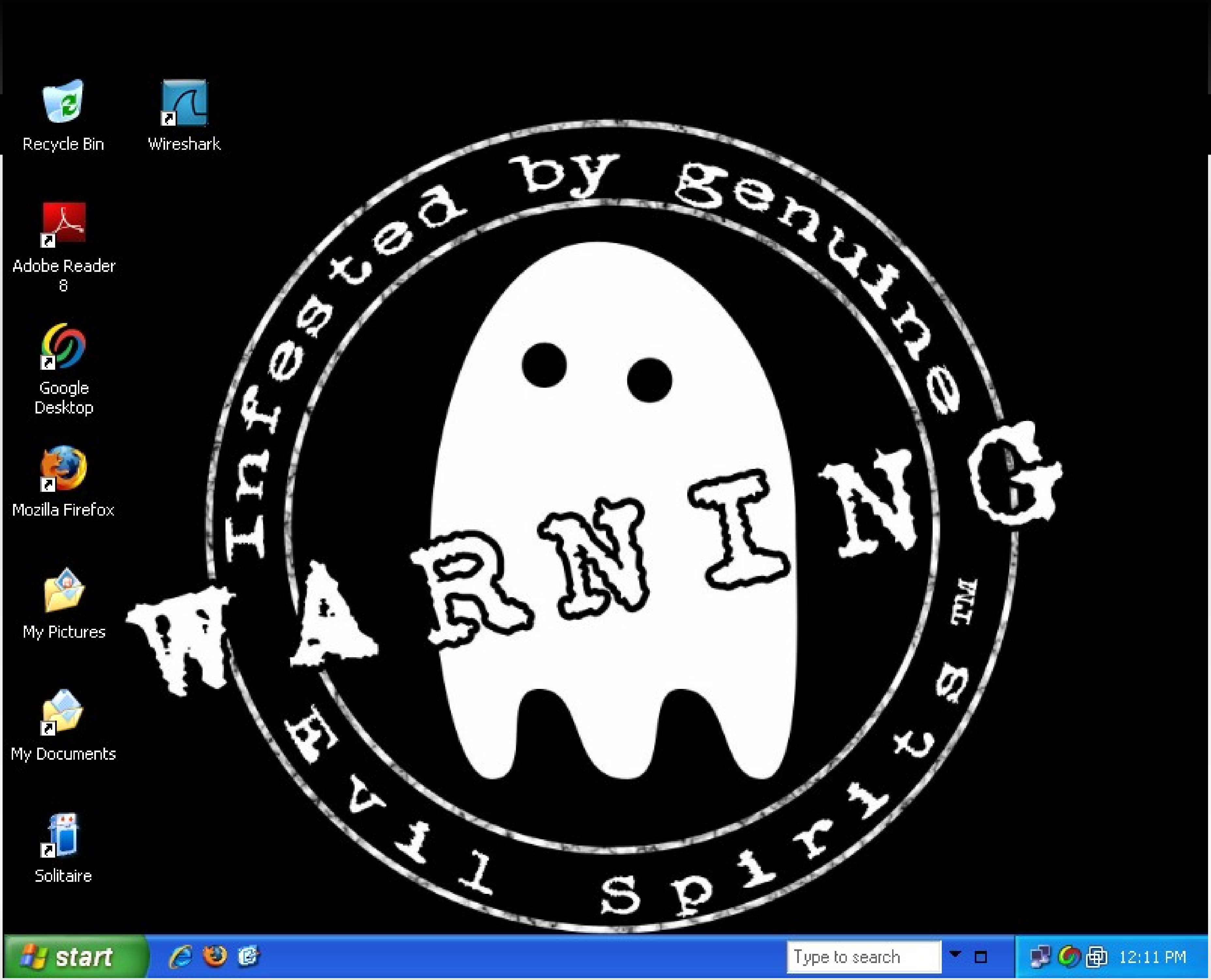
- Collecting memory data
- Techniques we considered using:
  - Crash dumps
  - Hibernation file
- Tool of choice:
  - FAU dd

# Collection: disk

- Collecting disk data
- Tools we considered using:
  - dd
  - sdd
- Tool of choice:
  - dcfldd

# Collection

- What happened onsite?



Recycle Bin
Wireshark
Adobe Reader 8
Google Desktop
Mozilla Firefox
My Pictures
My Documents
Solitaire
Infested by genuine
WARNING
Evil Spirits
TM
start
Type to search
12:11 PM

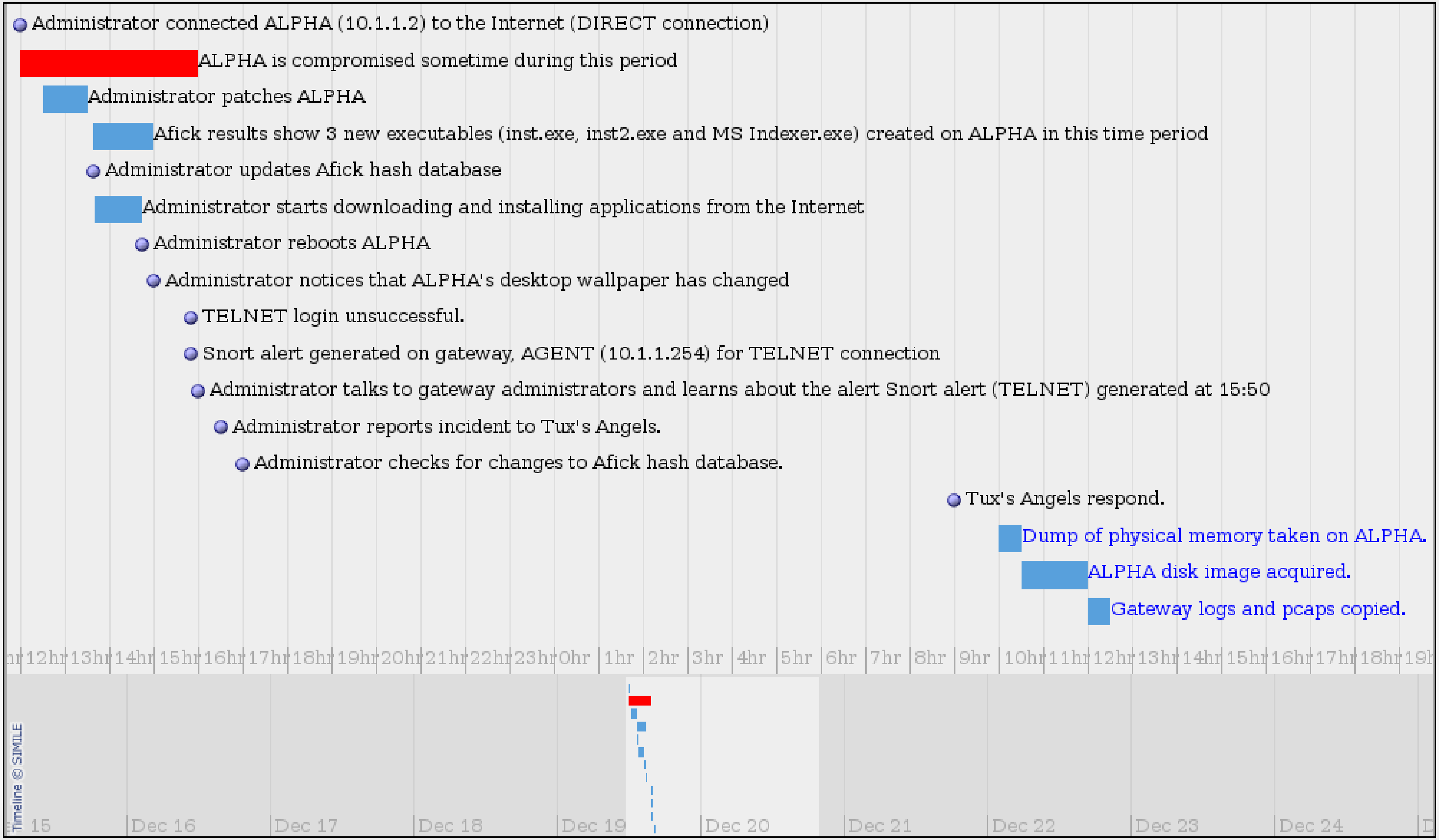
# Collection

- What happened onsite?
  - Physical memory: FAU dd and dcfldd
  - Disk image: dcfldd
  - Startup pcaps: tcpdump
  - Gateway pcaps: dumpcap

# DEMO:

## Memory acquisition using FAU dd and dcfldd

# Timeline + Collection: what we know



Administrator connected ALPHA (10.1.1.2) to the Internet (DIRECT connection)

ALPHA is compromised sometime during this period

Administrator patches ALPHA

Afick results show 3 new executables (inst.exe, inst2.exe and MS Indexer.exe) created on ALPHA in this time period

Administrator updates Afick hash database

Administrator starts downloading and installing applications from the Internet

Administrator reboots ALPHA

Administrator notices that ALPHA's desktop wallpaper has changed

TELNET login unsuccessful.

Snort alert generated on gateway, AGENT (10.1.1.254) for TELNET connection

Administrator talks to gateway administrators and learns about the alert Snort alert (TELNET) generated at 15:50

Administrator reports incident to Tux's Angels.

Administrator checks for changes to Afick hash database.

Tux's Angels respond.

Dump of physical memory taken on ALPHA.

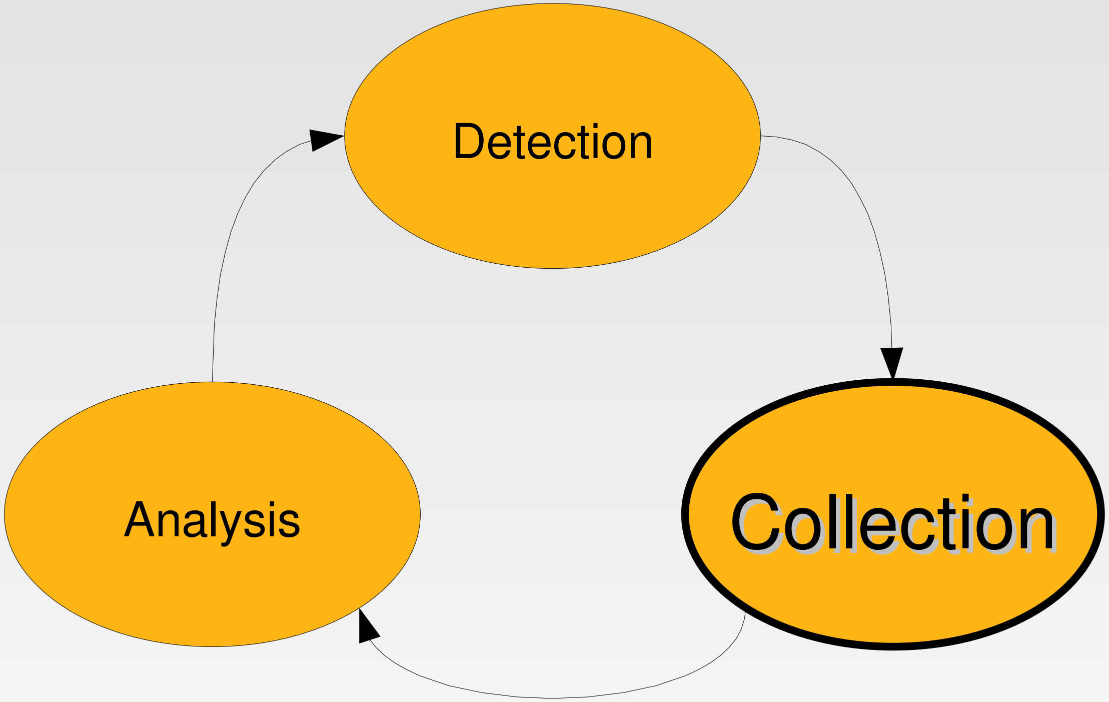
ALPHA disk image acquired.

Gateway logs and pcaps copied.

hr 12hr 13hr 14hr 15hr 16hr 17hr 18hr 19hr 20hr 21hr 22hr 23hr 0hr 1hr 2hr 3hr 4hr 5hr 6hr 7hr 8hr 9hr 10hr 11hr 12hr 13hr 14hr 15hr 16hr 17hr 18hr 19h
15 Dec 16 Dec 17 Dec 18 Dec 19 Dec 20 Dec 21 Dec 22 Dec 23 Dec 24 D
Timeline © SIMILE

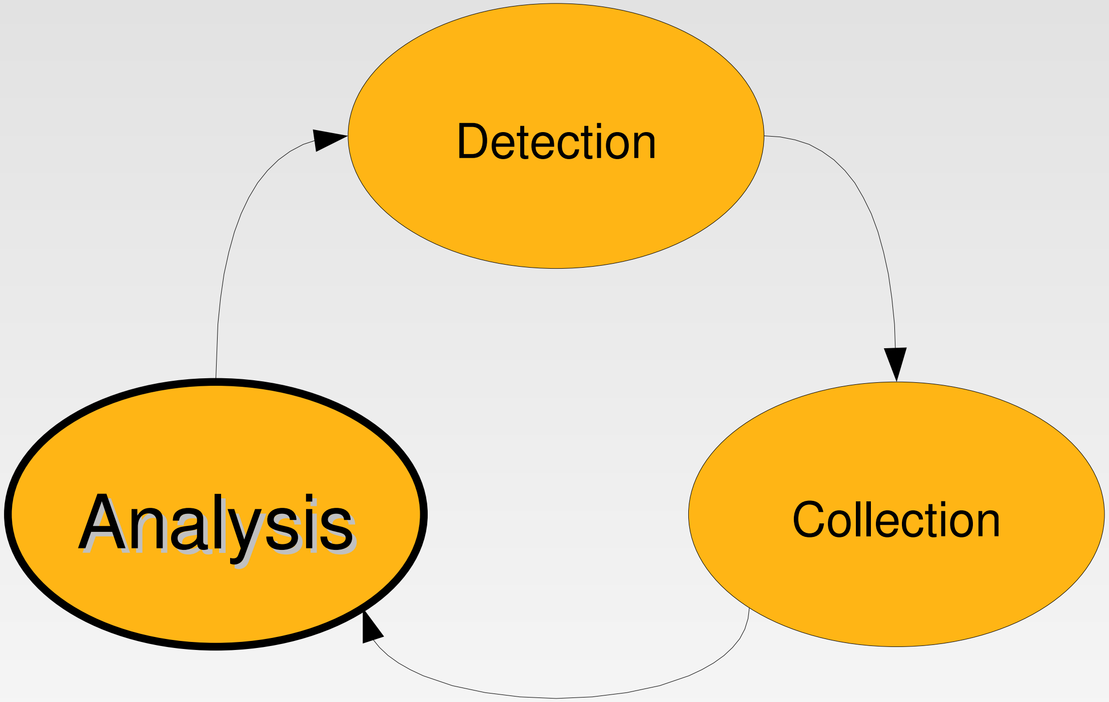
# Investigation

- The incident
- **IR life cycle**
  - Detection
  - **Collection**
  - Analysis



# Investigation

- The incident
- **IR life cycle**
  - Detection
  - Collection
  - **Analysis**



# Analysis

- Analysing the data acquired in collection phase
- Confirmatory analysis and event reconstruction
- Data is **S**urveyed, **E**xtracted and **E**xamined (SEE data analytic approach)

# Analysis

- Our priorities:
  1) Cause of compromise
  2) Extent of compromise
  3) Malware functionality & identity

# Analysis

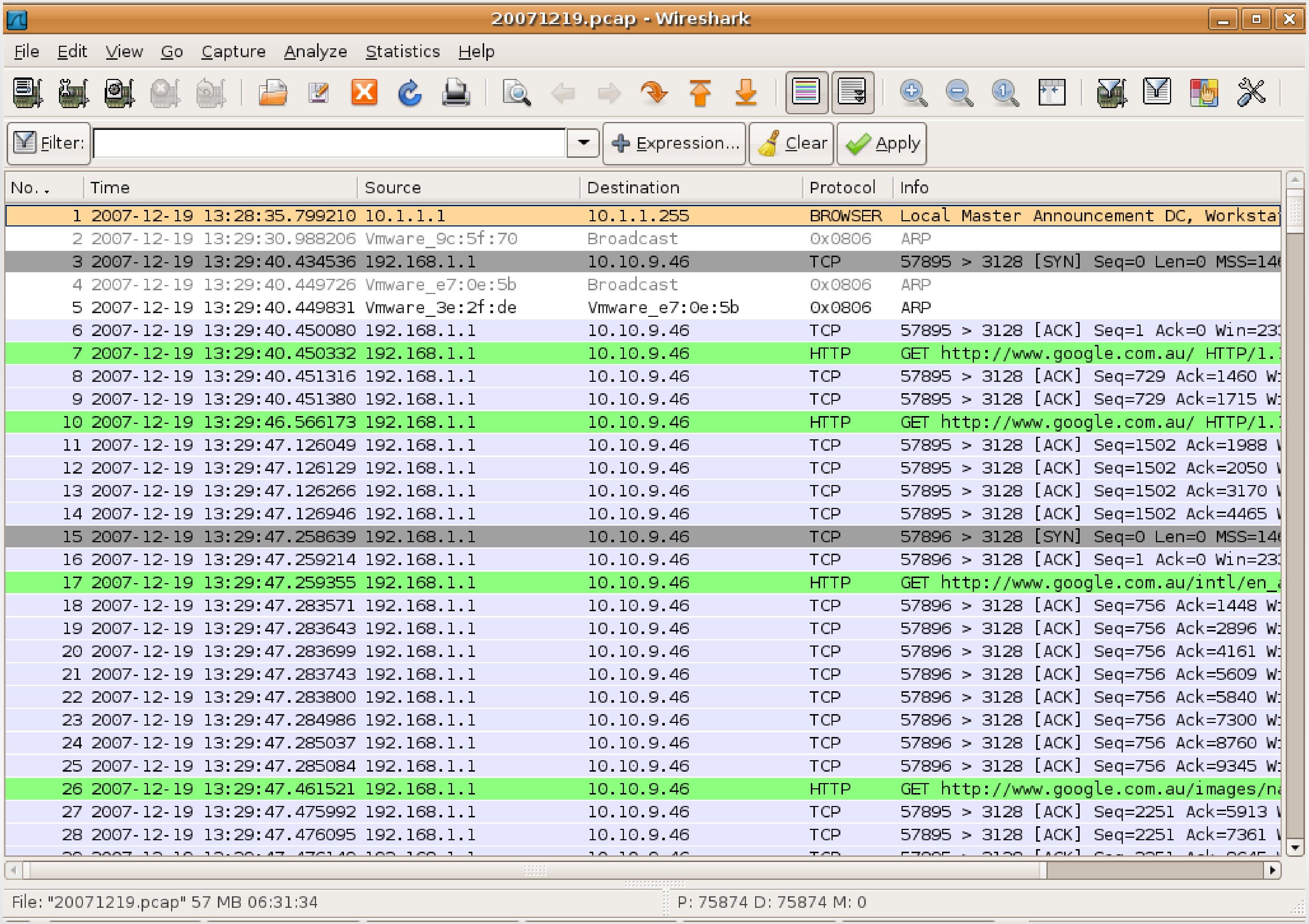
- Data from collection phase:
  - network
  - disk
  - memory
- Tools to analyse each dataset

# Analysis: network

# Analysis: network

- Network tools we considered:
  - tcpxtract
  - ngrep
  - netdude
- Our network tool of choice: wireshark

# Analysis: network



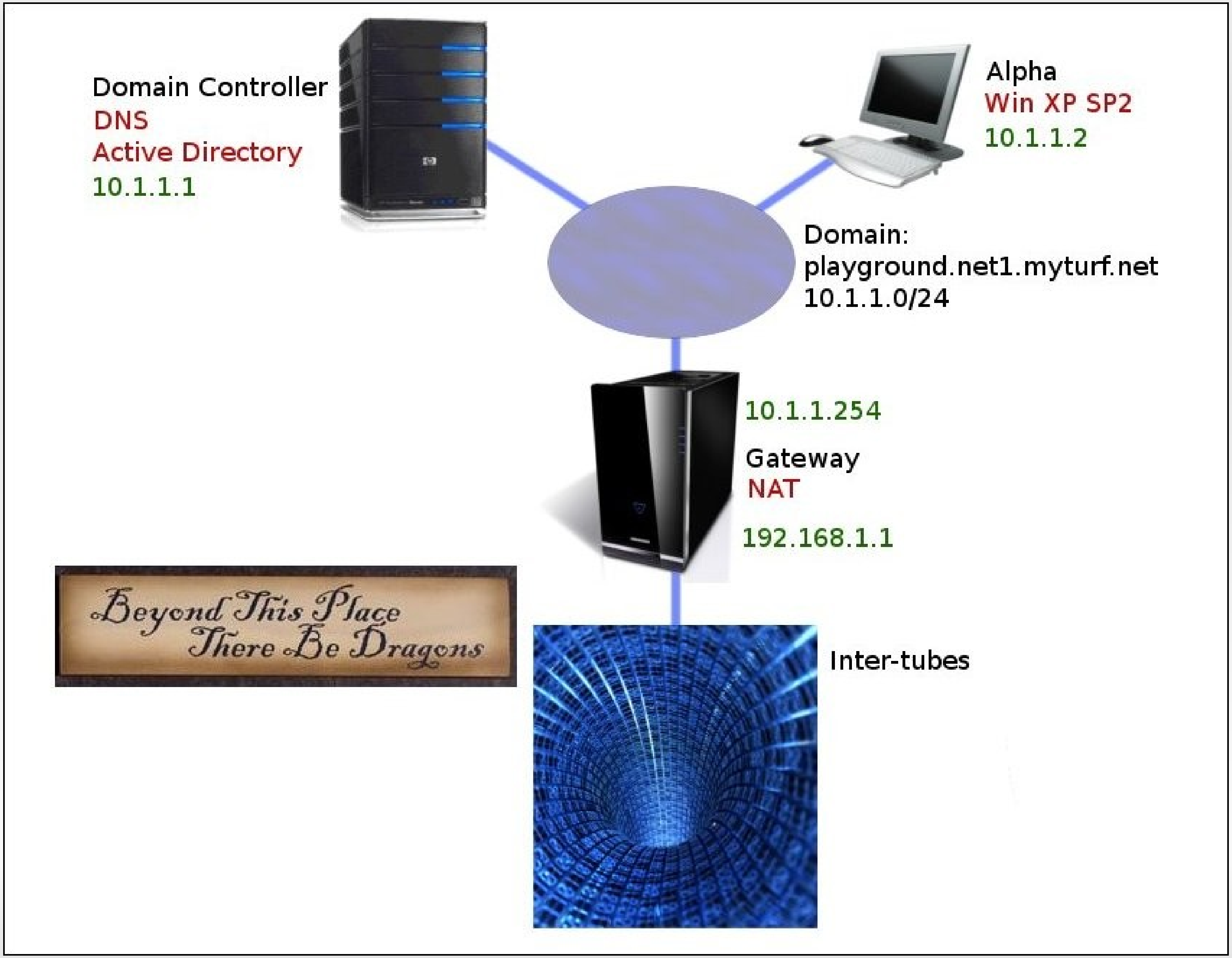
20071219.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression...
Clear
Apply

| No. . | Time | Source | Destination | Protocol | Info |
|---|---|---|---|---|---|
| 1 | 2007-12-19 13:28:35.799210 | 10.1.1.1 | 10.1.1.255 | BROWSER | Local Master Announcement DC, Workstat |
| 2 | 2007-12-19 13:29:30.988206 | Vmware_9c:5f:70 | Broadcast | 0x0806 | ARP |
| 3 | 2007-12-19 13:29:40.434536 | 192.168.1.1 | 10.10.9.46 | TCP | 57895 > 3128 [SYN] Seq=0 Len=0 MSS=14 |
| 4 | 2007-12-19 13:29:40.449726 | Vmware_e7:0e:5b | Broadcast | 0x0806 | ARP |
| 5 | 2007-12-19 13:29:40.449831 | Vmware_3e:2f:de | Vmware_e7:0e:5b | 0x0806 | ARP |
| 6 | 2007-12-19 13:29:40.450080 | 192.168.1.1 | 10.10.9.46 | TCP | 57895 > 3128 [ACK] Seq=1 Ack=0 Win=23 |
| 7 | 2007-12-19 13:29:40.450332 | 192.168.1.1 | 10.10.9.46 | HTTP | GET http://www.google.com.au/ HTTP/1. |
| 8 | 2007-12-19 13:29:40.451316 | 192.168.1.1 | 10.10.9.46 | TCP | 57895 > 3128 [ACK] Seq=729 Ack=1460 W |
| 9 | 2007-12-19 13:29:40.451380 | 192.168.1.1 | 10.10.9.46 | TCP | 57895 > 3128 [ACK] Seq=729 Ack=1715 W |
| 10 | 2007-12-19 13:29:46.566173 | 192.168.1.1 | 10.10.9.46 | HTTP | GET http://www.google.com.au/ HTTP/1. |
| 11 | 2007-12-19 13:29:47.126049 | 192.168.1.1 | 10.10.9.46 | TCP | 57895 > 3128 [ACK] Seq=1502 Ack=1988 W |
| 12 | 2007-12-19 13:29:47.126129 | 192.168.1.1 | 10.10.9.46 | TCP | 57895 > 3128 [ACK] Seq=1502 Ack=2050 W |
| 13 | 2007-12-19 13:29:47.126266 | 192.168.1.1 | 10.10.9.46 | TCP | 57895 > 3128 [ACK] Seq=1502 Ack=3170 W |
| 14 | 2007-12-19 13:29:47.126946 | 192.168.1.1 | 10.10.9.46 | TCP | 57895 > 3128 [ACK] Seq=1502 Ack=4465 W |
| 15 | 2007-12-19 13:29:47.258639 | 192.168.1.1 | 10.10.9.46 | TCP | 57896 > 3128 [SYN] Seq=0 Len=0 MSS=14 |
| 16 | 2007-12-19 13:29:47.259214 | 192.168.1.1 | 10.10.9.46 | TCP | 57896 > 3128 [ACK] Seq=1 Ack=0 Win=23 |
| 17 | 2007-12-19 13:29:47.259355 | 192.168.1.1 | 10.10.9.46 | HTTP | GET http://www.google.com.au/intl/en_ |
| 18 | 2007-12-19 13:29:47.283571 | 192.168.1.1 | 10.10.9.46 | TCP | 57896 > 3128 [ACK] Seq=756 Ack=1448 W |
| 19 | 2007-12-19 13:29:47.283643 | 192.168.1.1 | 10.10.9.46 | TCP | 57896 > 3128 [ACK] Seq=756 Ack=2896 W |
| 20 | 2007-12-19 13:29:47.283699 | 192.168.1.1 | 10.10.9.46 | TCP | 57896 > 3128 [ACK] Seq=756 Ack=4161 W |
| 21 | 2007-12-19 13:29:47.283743 | 192.168.1.1 | 10.10.9.46 | TCP | 57896 > 3128 [ACK] Seq=756 Ack=5609 W |
| 22 | 2007-12-19 13:29:47.283800 | 192.168.1.1 | 10.10.9.46 | TCP | 57896 > 3128 [ACK] Seq=756 Ack=5840 W |
| 23 | 2007-12-19 13:29:47.284986 | 192.168.1.1 | 10.10.9.46 | TCP | 57896 > 3128 [ACK] Seq=756 Ack=7300 W |
| 24 | 2007-12-19 13:29:47.285037 | 192.168.1.1 | 10.10.9.46 | TCP | 57896 > 3128 [ACK] Seq=756 Ack=8760 W |
| 25 | 2007-12-19 13:29:47.285084 | 192.168.1.1 | 10.10.9.46 | TCP | 57896 > 3128 [ACK] Seq=756 Ack=9345 W |
| 26 | 2007-12-19 13:29:47.461521 | 192.168.1.1 | 10.10.9.46 | HTTP | GET http://www.google.com.au/images/na |
| 27 | 2007-12-19 13:29:47.475992 | 192.168.1.1 | 10.10.9.46 | TCP | 57895 > 3128 [ACK] Seq=2251 Ack=5913 W |
| 28 | 2007-12-19 13:29:47.476095 | 192.168.1.1 | 10.10.9.46 | TCP | 57895 > 3128 [ACK] Seq=2251 Ack=7361 W |

File: "20071219.pcap" 57 MB 06:31:34

P: 75874 D: 75874 M: 0

# The network

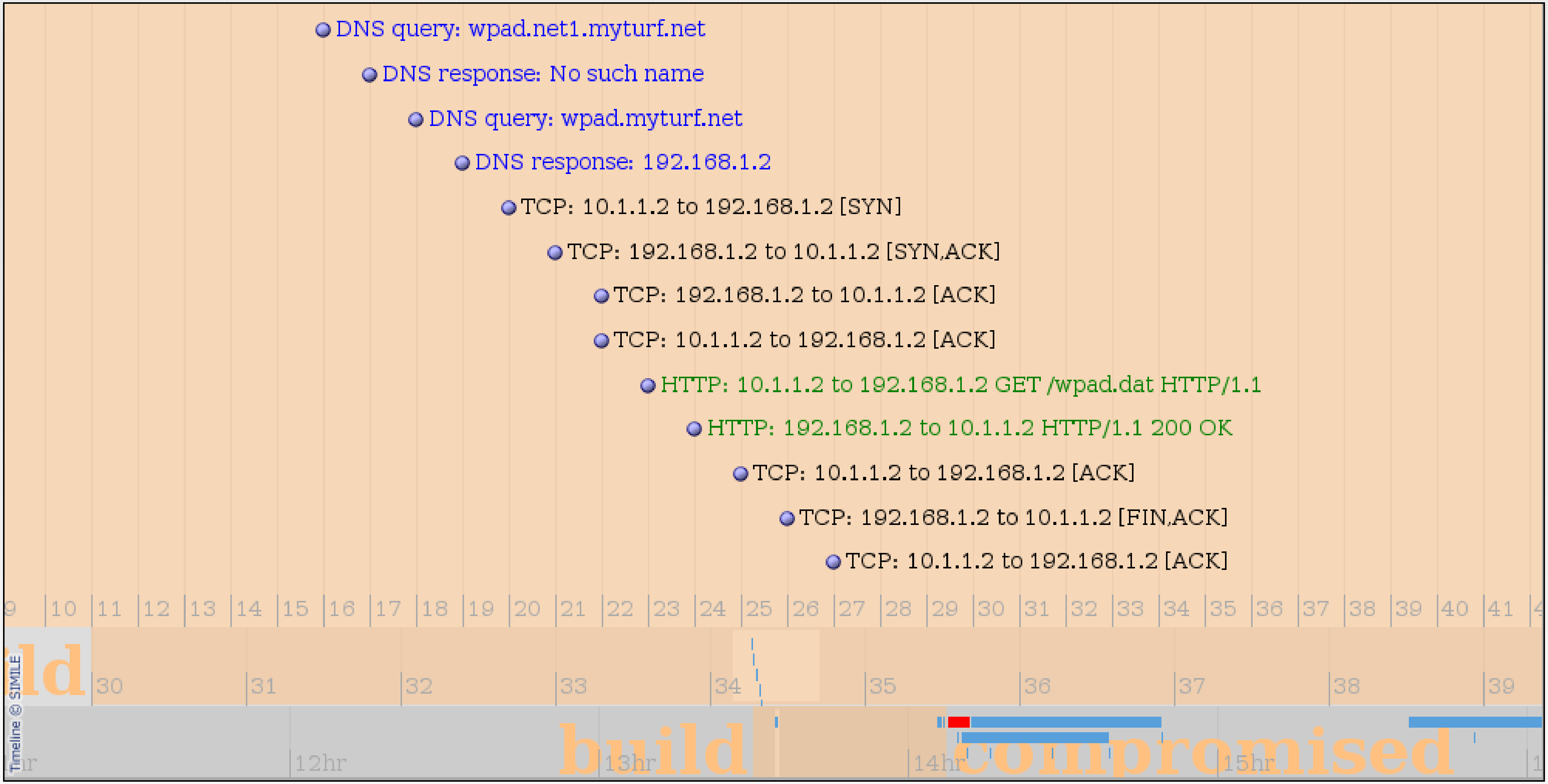

Domain Controller
DNS
Active Directory
10.1.1.1
Alpha
Win XP SP2
10.1.1.2
Domain:
playground.net1.myturf.net
10.1.1.0/24
10.1.1.254
Gateway
NAT
192.168.1.1
Beyond This Place
There Be Dragons
Inter-tubes

# Analysis: network

- Network capture (20071219.pcap):
  - From 2007-12-19 13:28 to 2007-12-19 20:00
  - Taken on external gateway interface (192.168.1.1)
- First observation:
  - At 14:05 ALPHA starts using a proxy rather than a DIRECT connection to the Internet
  - Proxy is an untrusted IP address: 192.168.1.2

# Timeline: wpad DNS request

# Timeline: wpad DNS request



DNS query: wpad.net1.myturf.net

DNS response: No such name

DNS query: wpad.myturf.net

DNS response: 192.168.1.2

TCP: 10.1.1.2 to 192.168.1.2 [SYN]

TCP: 192.168.1.2 to 10.1.1.2 [SYN,ACK]

TCP: 192.168.1.2 to 10.1.1.2 [ACK]

TCP: 10.1.1.2 to 192.168.1.2 [ACK]

HTTP: 10.1.1.2 to 192.168.1.2 GET /wpad.dat HTTP/1.1

HTTP: 192.168.1.2 to 10.1.1.2 HTTP/1.1 200 OK

TCP: 10.1.1.2 to 192.168.1.2 [ACK]

TCP: 192.168.1.2 to 10.1.1.2 [FIN,ACK]

TCP: 10.1.1.2 to 192.168.1.2 [ACK]

# Analysis: wpad.dat

```
function FindProxyForURL(url, host)
{
  if (shExpMatch(url, "*.playground.net1.myturf.net/*"))
  {
    return "DIRECT";
  }

  return "PROXY proxy.myturf.net:3128";
}
```

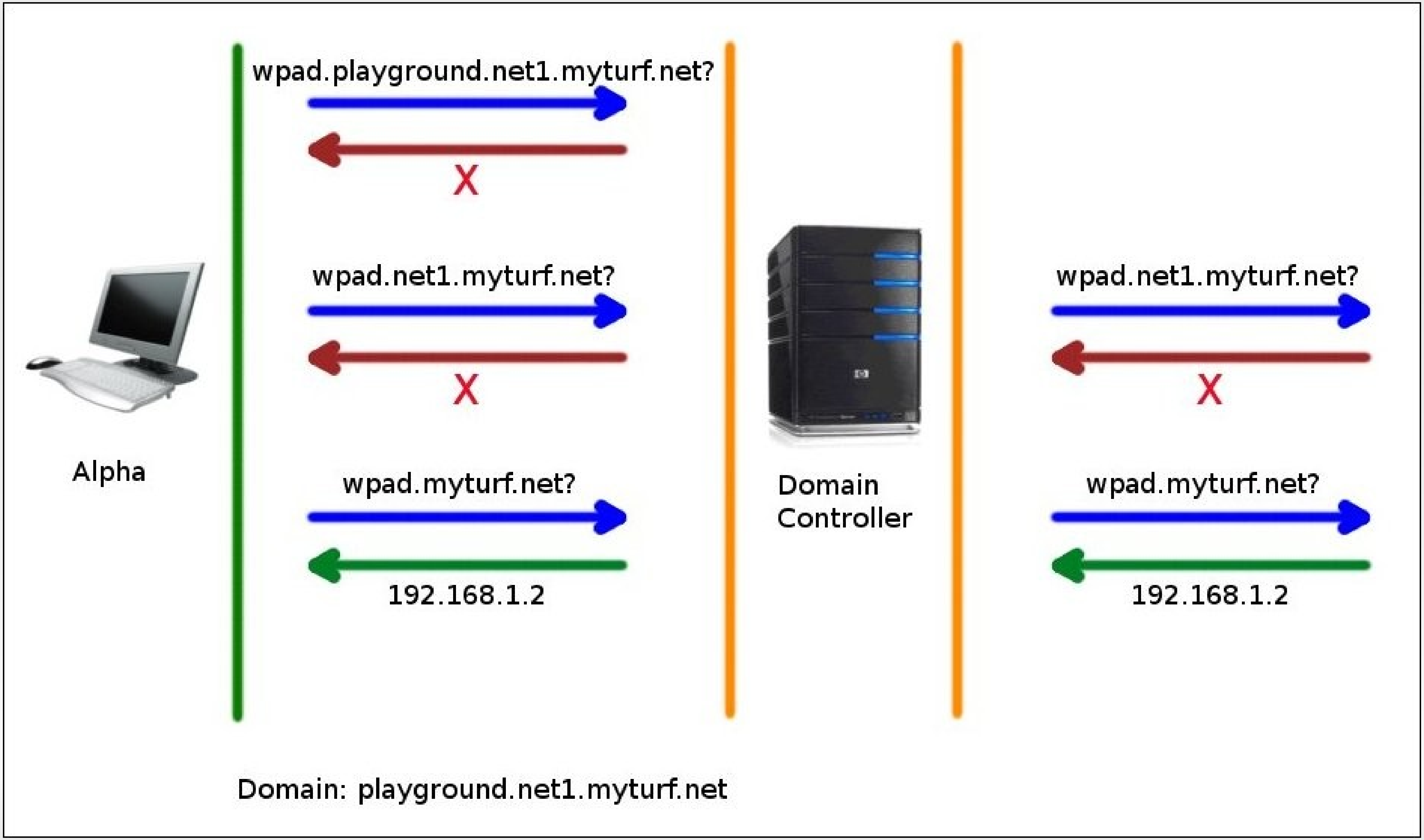
# Analysis: wpad.dat

```
function FindProxyForURL(url, host)
{
  if (shExpMatch(url, "*.playground.net1.myturf.net/*"))
  {
    return "DIRECT";
  }

  return "PROXY proxy.myturf.net:3128";
}
```

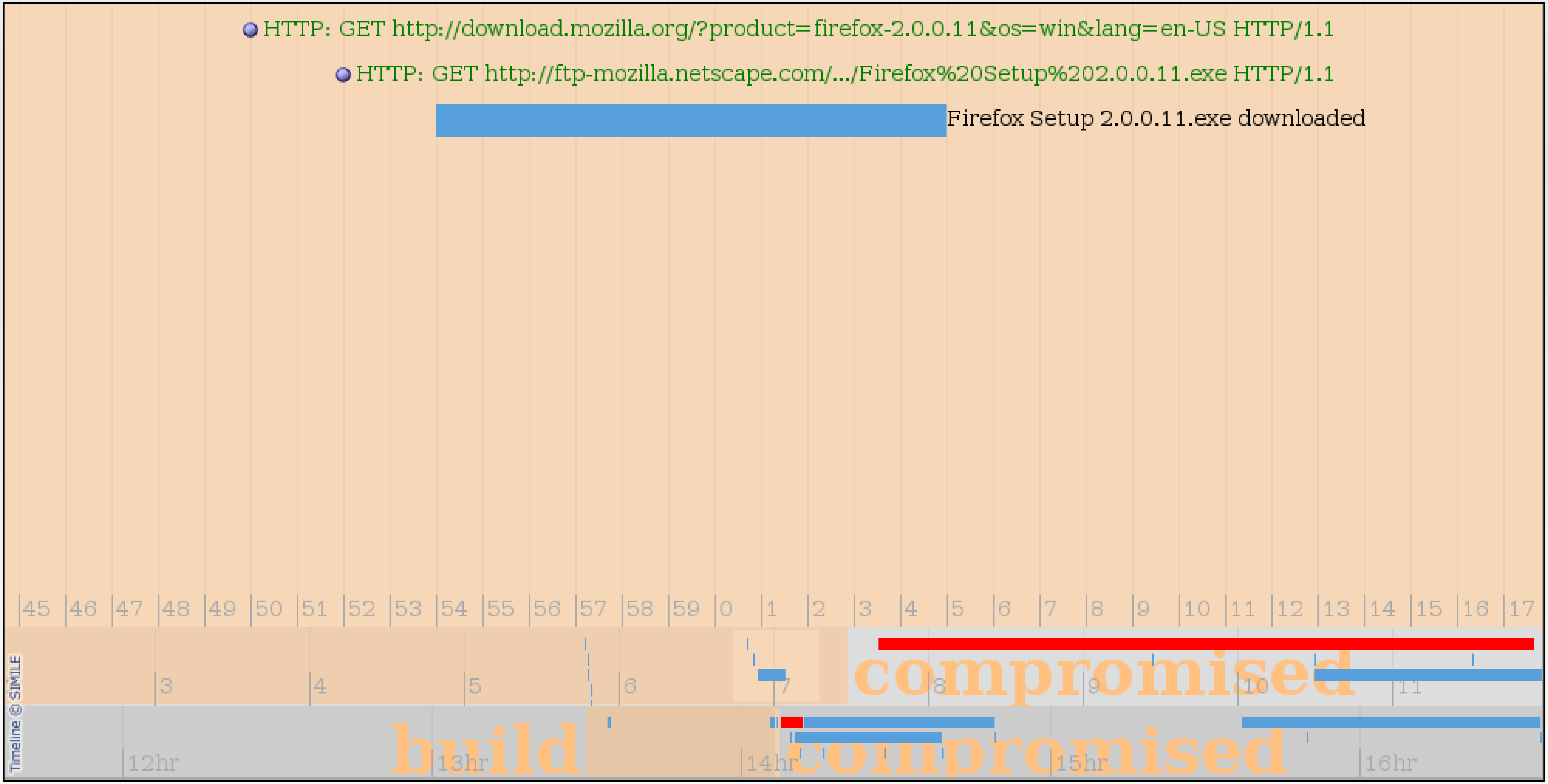
# Analysis: wpad refresher

- **W**eb **P**roxy **A**uto**d**iscovery protocol
- Used by web browsers set to ”auto-detect proxy settings”
- DHCP and **DNS**
- **wpad**.<domain>
- Moves up hierarchy until it gets a hit

# Analysis: wpad resolving



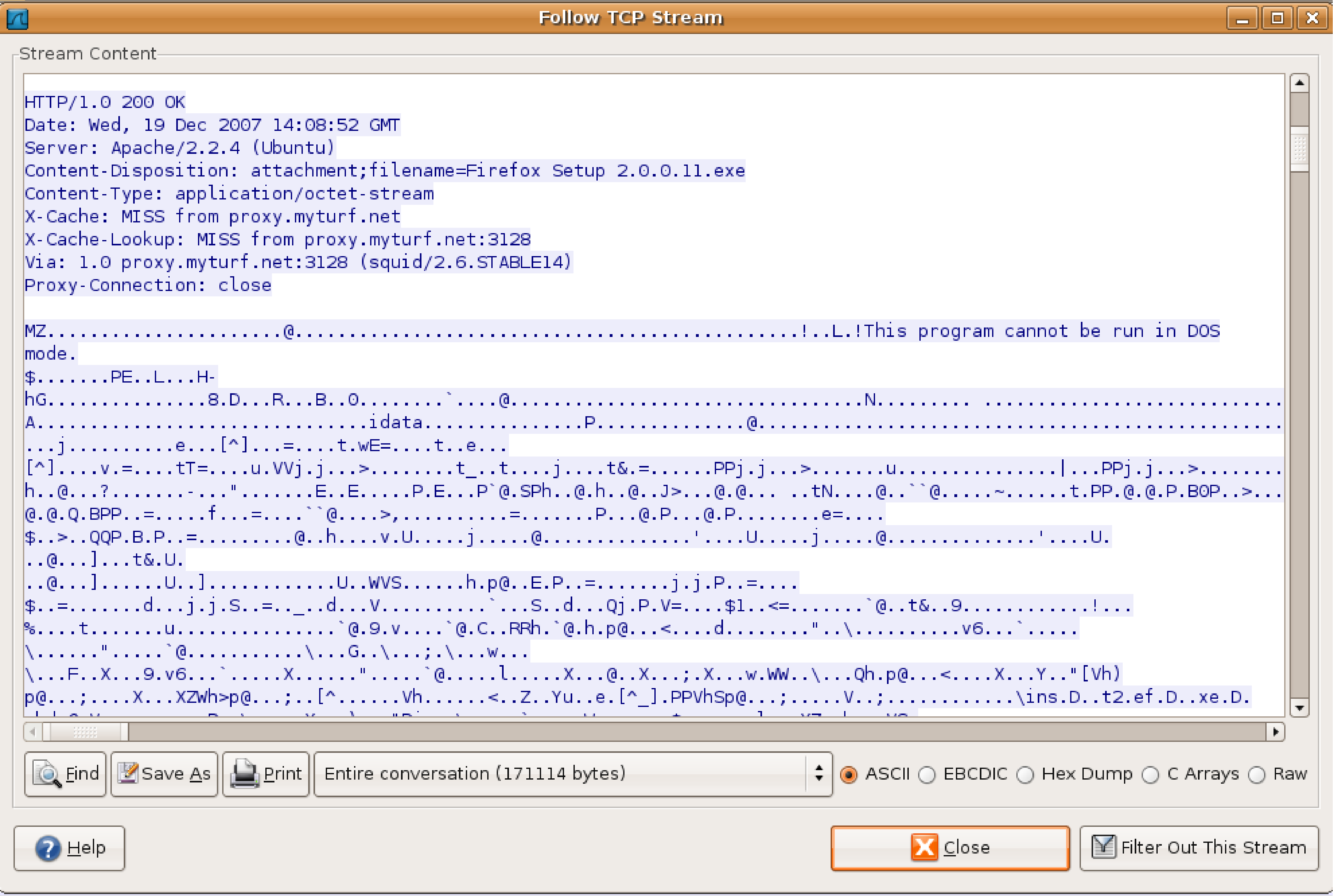
# Timeline: Firefox setup.exe downloaded



HTTP: GET http://download.mozilla.org/?product=firefox-2.0.0.11&os=win&lang=en-US HTTP/1.1

HTTP: GET http://ftp-mozilla.netscape.com/.../Firefox%20Setup%202.0.0.11.exe HTTP/1.1

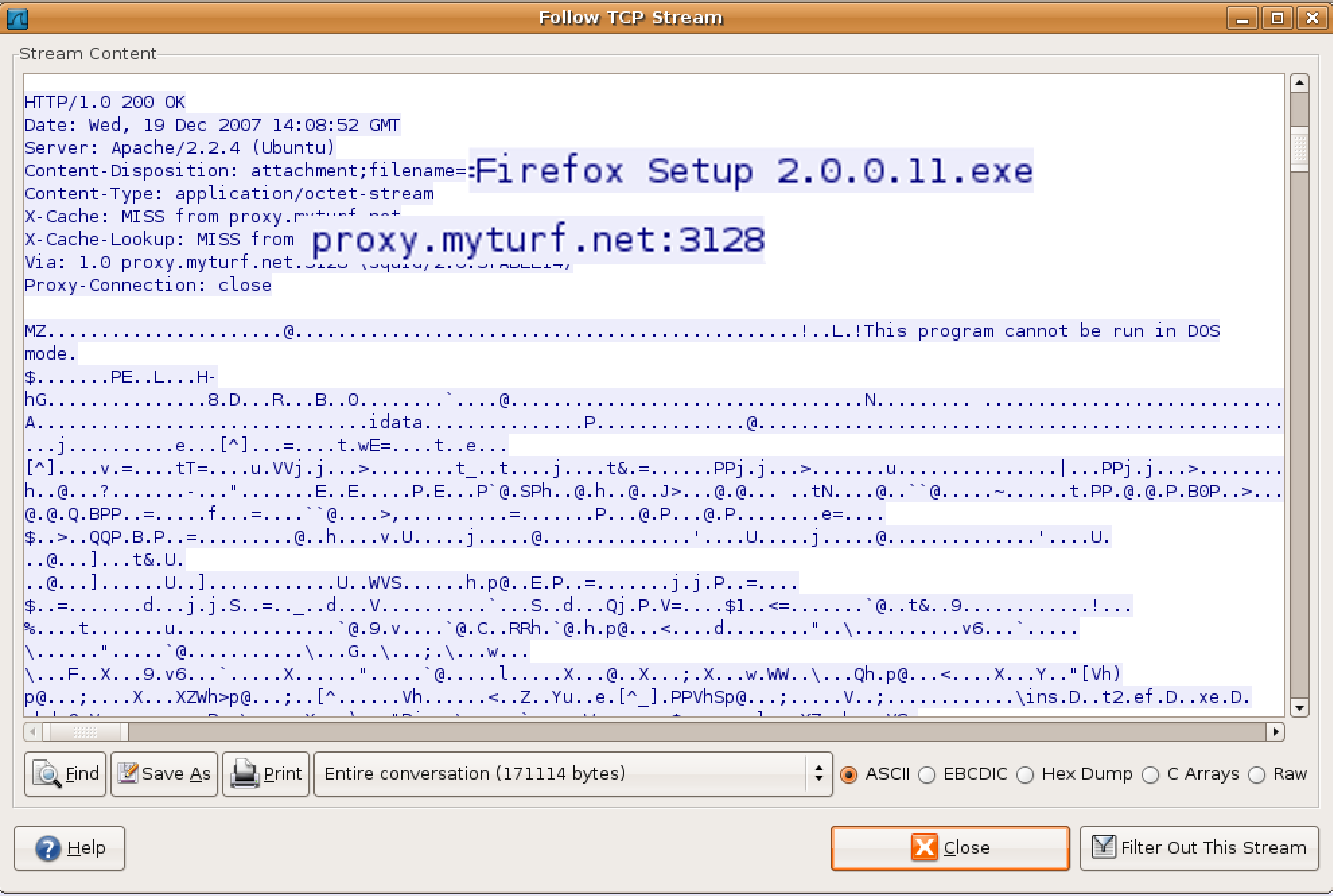
Firefox Setup 2.0.0.11.exe downloaded



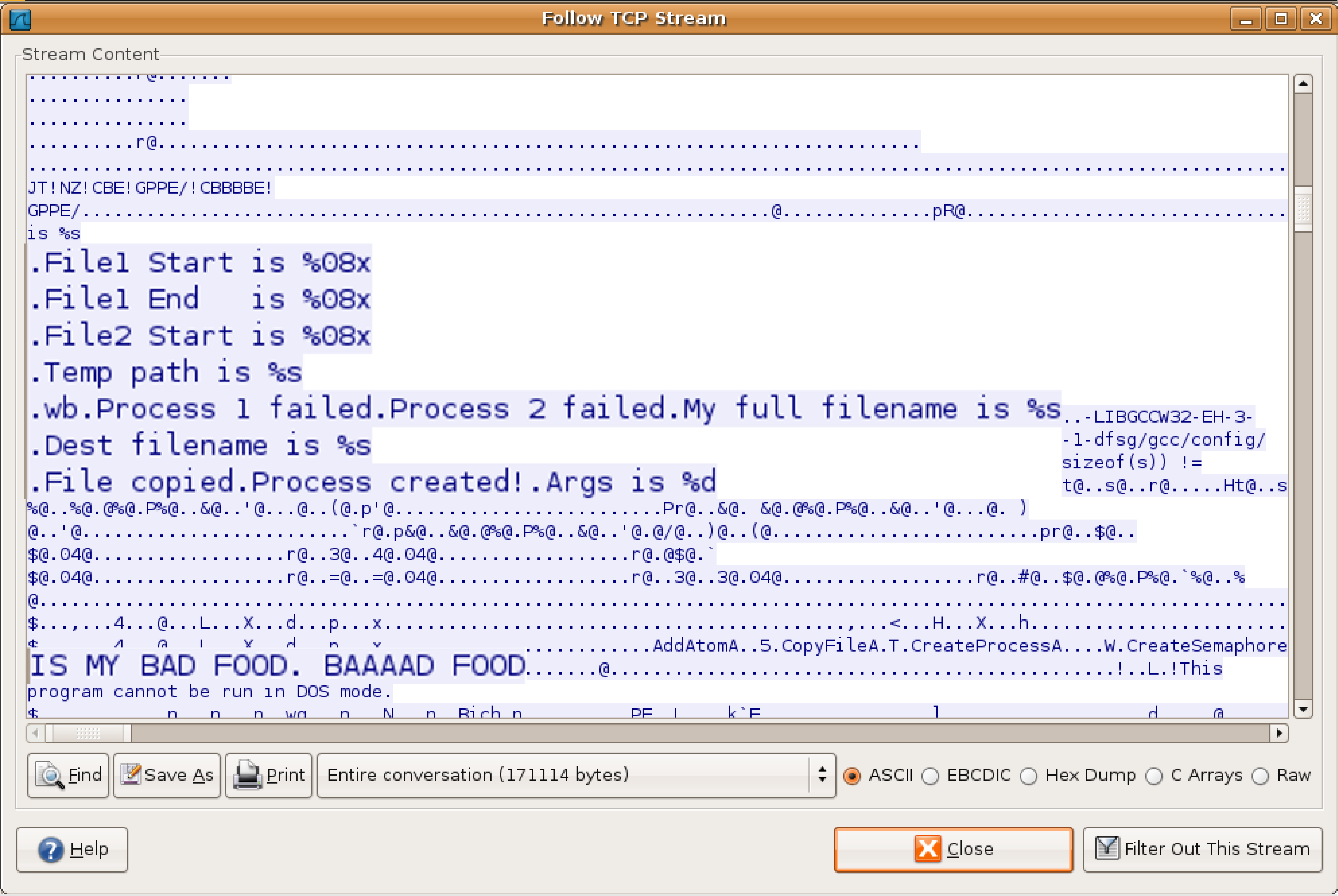
```
HTTP/1.0 200 OK
Date: Wed, 19 Dec 2007 14:08:52 GMT
Server: Apache/2.2.4 (Ubuntu)
Content-Disposition: attachment;filename=Firefox Setup 2.0.0.11.exe
Content-Type: application/octet-stream
X-Cache: MISS from proxy.myturf.net
X-Cache-Lookup: MISS from proxy.myturf.net:3128
Via: 1.0 proxy.myturf.net:3128 (squid/2.6.STABLE14)
Proxy-Connection: close

MZ.......................@..........................................!..L.!This program cannot be run in DOS
mode.
$.......PE..L...H-
hG...............8.D...R...B..O........`....@...............................N.........  .......................
A..............................idata..............P..............@...........................................
...j..........e...[^]...=....t.wE=....t..e...
[^]....v.=....tT=....u.VVj.j...>........t_..t....j....t&.=......PPj.j...>.......u................|...PPj.j...>.......
h..@...?.......-..."........E..E.....P.E...P`@.SPh..@.h..@..J>...@.@...  ..tN....@..``@.....~......t.PP.@.@.P.BOP..>...
@.@.Q.BPP..=.....f...=....``@....>,..........=.......P...@.P...@.P........e=....
$..>..QQP.B.P..=.........@..h....v.U....j.....@..............'....U....j.....@..............'....U.
..@...]...t&.U.
..@...]......U..]............U..WVS......h.p@..E.P..=.......j.j.P..=....
$..=.......d...j.j.S..=.._..d...V..........`...S..d...Qj.P.V=....$1..<=.......`@..t&..9............!...
%....t.......u................`@.9.v....`@.C..RRh.`@.h.p@...<....d........"..\..........v6...`.....
\......".....`@...........\...G..\...;.\...w...
\...F..X...9.v6...`.....X......".....`@.....l.....X...@..X...;.X...w.WW..\...Qh.p@...<....X...Y.."[Vh)
p@...;....X...XZWh>p@...;..[^......Vh......<..Z..Yu..e.[^_].PPVhSp@...;.....V..;.............\ins.D..t2.ef.D..xe.D.
```

Entire conversation (171114 bytes)

● ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ○ Raw


Follow TCP Stream
Stream Content
Find
Save As
Print
Entire conversation (171114 bytes)
● ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ○ Raw
Help
Close
Filter Out This Stream

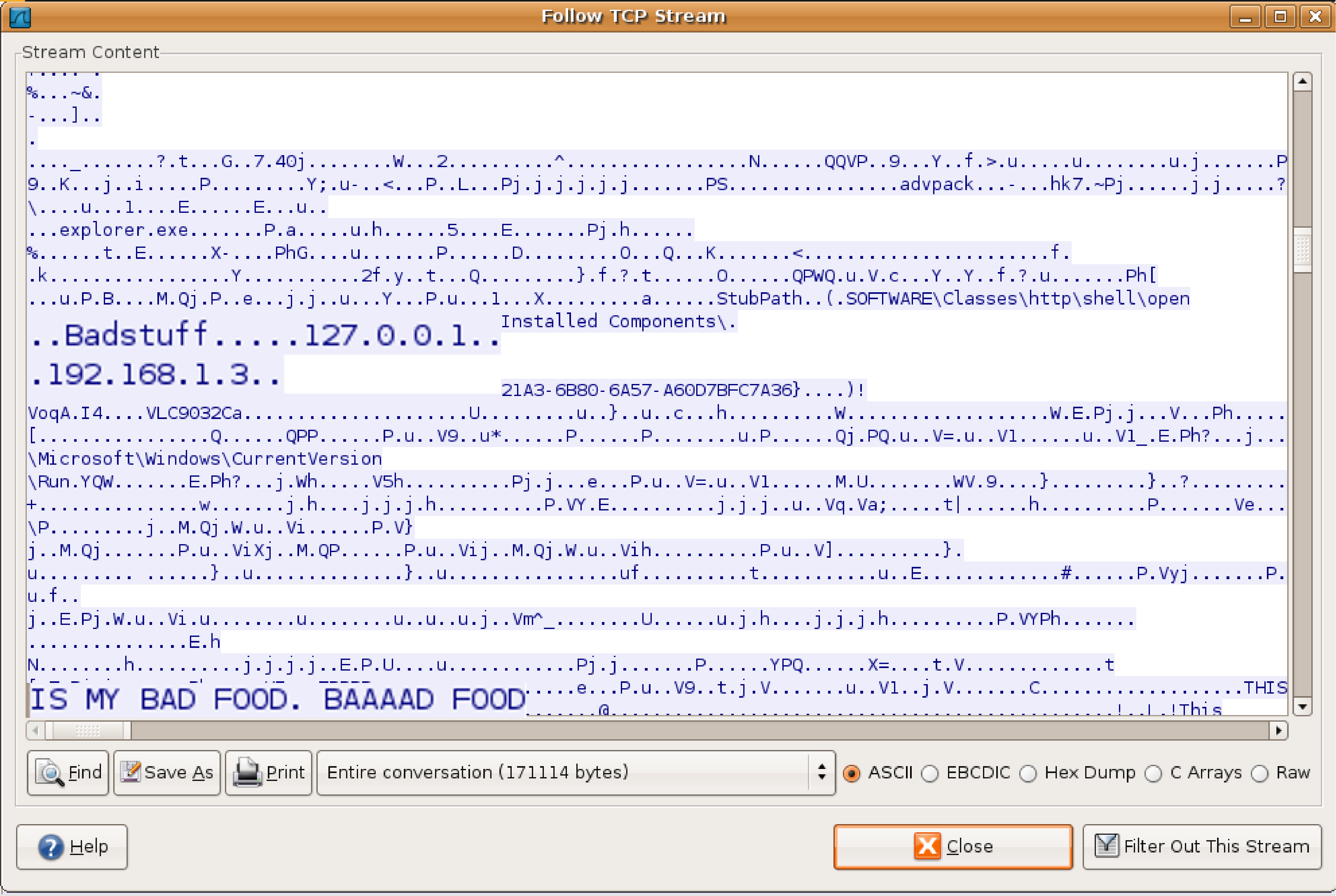
```
HTTP/1.0 200 OK
Date: Wed, 19 Dec 2007 14:08:52 GMT
Server: Apache/2.2.4 (Ubuntu)
Content-Disposition: attachment;filename=Firefox Setup 2.0.0.11.exe
Content-Type: application/octet-stream
X-Cache: MISS from proxy.myturf.net
X-Cache-Lookup: MISS from proxy.myturf.net:3128
Via: 1.0 proxy.myturf.net:3128 (squid/2.6.STABLE14)
Proxy-Connection: close

MZ.......................@..............................................!..L.!This program cannot be run in DOS
mode.
$.......PE..L...H-
hG..............8.D...R...B..0........`....@................................N.........  ......................
A..............................idata...............P..............@........................................
...j..........e...[^]...=....t.wE=....t..e...
[^]....v.=....tT=....u.VVj.j...>.........t_..t....j....t&.=......PPj.j...>.......u.................|...PPj.j...>.......
h..@...?.......-..."........E..E.....P.E...P`@.SPh..@.h..@..J>...@.@...  ..tN....@..``@.....~.......t.PP.@.@.P.BOP..>...
@.@.Q.BPP..=.....f...=....``@....>,.........=.......P...@.P...@.P.........e=....
$..>..QQP.B.P..=.........@..h....v.U....j.....@..............'....U....j.....@...............'....U.
..@...]...t&.U.
..@...]......U..]...........U..WVS......h.p@..E.P..=.......j.j.P..=....
$..=.......d...j.j.S..=.._..d...V..........`...S..d...Qj.P.V=....$1..<=.......`@..t&..9.............!...
%....t.......u................`@.9.v....`@.C..RRh.`@.h.p@...<....d........"..\...........v6...`.....
\......"......`@...........\...G..\...;.\...w...
\...F..X...9.v6...`......X......"......`@.....l.....X...@..X...;.X...w.WW..\...Qh.p@...<....X...Y.."[Vh)
p@...;....X...XZWh>p@...;..[^......Vh......<..Z..Yu..e.[^_].PPVhSp@...;.....V..;.............\ins.D..t2.ef.D..xe.D.
```



```
..........'@.......
..............
..............
..........r@..................................................................
.......................................................................................................
JT!NZ!CBE!GPPE/!CBBBBE!
GPPE/...............................................................@..............pR@............................
is %s
.File1 Start is %08x
.File1 End   is %08x
.File2 Start is %08x
.Temp path is %s
.wb.Process 1 failed.Process 2 failed.My full filename is %s..-LIBGCCW32-EH-3-
                                                             -1-dfsg/gcc/config/
.Dest filename is %s
                                                             sizeof(s)) !=
.File copied.Process created!.Args is %d                     t@..s@..r@.....Ht@..s
%@..%@.@%@.P%@..&@..'@...@..(@.p'@........................Pr@..&@. &@.@%@.P%@..&@..'@...@. )
@..'@.......................`r@.p&@..&@.@%@.P%@..&@..'@.@/@..)@..(@.........................pr@..$@..
$@.04@.................r@..3@..4@.04@.................r@.@$@.`
$@.04@.................r@..=@..=@.04@.................r@..3@..3@.04@.................r@..#@..$@.@%@.P%@.`%@..%
@.......................................................................................................
$...,...4...@...L...X...d...p...x...........................,...<...H...X...h..........................
$....4...@...L...X...d...p...x............AddAtomA..5.CopyFileA.T.CreateProcessA....W.CreateSemaphore
IS MY BAD FOOD. BAAAAD FOOD......@.............................................!..L.!This
program cannot be run in DOS mode.
$...............n...n...n..wq...n...N...n..Rich.n...........PE..L.....k`E...............l...............d.....@
```

Entire conversation (171114 bytes)

● ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ○ Raw



```
%...~&.
-...]..
.
...._.......?.t...G..7.40j........W...2..........^................N......QQVP..9...Y..f.>.u.....u.........u.j.......P
9..K...j..i.....P.........Y;.u-..<...P..L...Pj.j.j.j.j.j.......PS................advpack...-...hk7.~Pj......j.j.....?
\....u...l....E......E...u..
...explorer.exe.......P.a.....u.h......5....E.......Pj.h......
%......t..E......X-....PhG....u.......P......D.........O...Q...K.......<.......................f.
.k.................Y...........2f.y..t...Q.........}.f.?.t......O......QPWQ.u.V.c...Y..Y..f.?.u.......Ph[
...u.P.B....M.Qj.P..e...j.j..u...Y...P.u...l...X.........a......StubPath..(.SOFTWARE\Classes\http\shell\open
..Badstuff......127.0.0.1.. Installed Components\.
.192.168.1.3..
                                21A3-6B80-6A57-A60D7BFC7A36}....)!
VoqA.I4....VLC9032Ca.....................U..........u..}..u..c...h..........W..................W.E.Pj.j...V...Ph.....
[................Q......QPP......P.u..V9..u*......P......P........u.P......Qj.PQ.u..V=.u..Vl......u..Vl_.E.Ph?...j...
\Microsoft\Windows\CurrentVersion
\Run.YQW.......E.Ph?...j.Wh.....V5h..........Pj.j...e...P.u..V=.u..Vl......M.U........WV.9....}.........}..?.........
+..............w.......j.h....j.j.j.h..........P.VY.E..........j.j.j..u..Vq.Va;.....t|......h..........P.......Ve...
\P.........j..M.Qj.W.u..Vi......P.V}
j..M.Qj.......P.u..ViXj..M.QP......P.u..Vij..M.Qj.W.u..Vih..........P.u..V]..........}.
u........ ......}..u..............}..u................uf..........t...........u..E.............#......P.Vyj.......P.
u.f..
j..E.Pj.W.u..Vi.u.........u.........u..u..u.j..Vm^_........U......u.j.h....j.j.j.h..........P.VYPh.......
...............E.h
N........h..........j.j.j.j..E.P.U....u.............Pj.j.......P......YPQ......X=....t.V..............t
IS MY BAD FOOD. BAAAAD FOOD.....e...P.u..V9..t.j.V........u..Vl..j.V.......C.....................THIS
                           .......@.......................................!..L.!This
```

Entire conversation (171114 bytes)

● ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ○ Raw

# Analysis: network

- Is this the real firefox setup.exe?

# Analysis: network

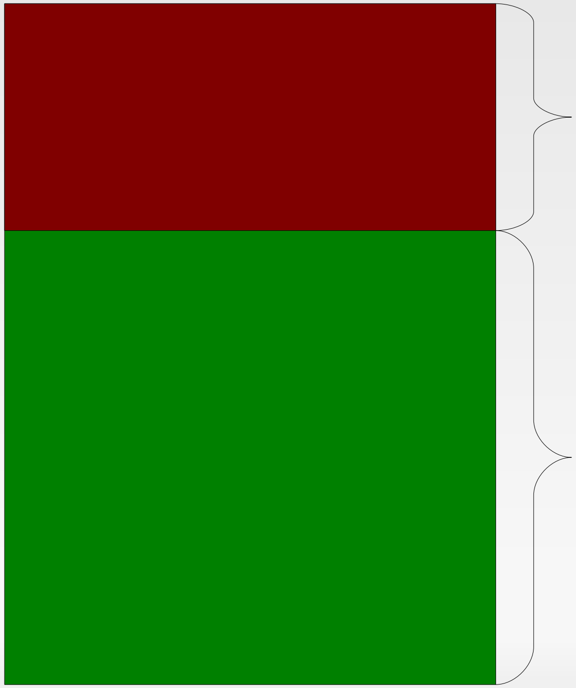
- Is this the real firefox setup.exe? NO WAY!

# Analysis: network

- Is this the real firefox setup.exe? NO WAY!
- Content-type: application/octet-stream

# Analysis: network

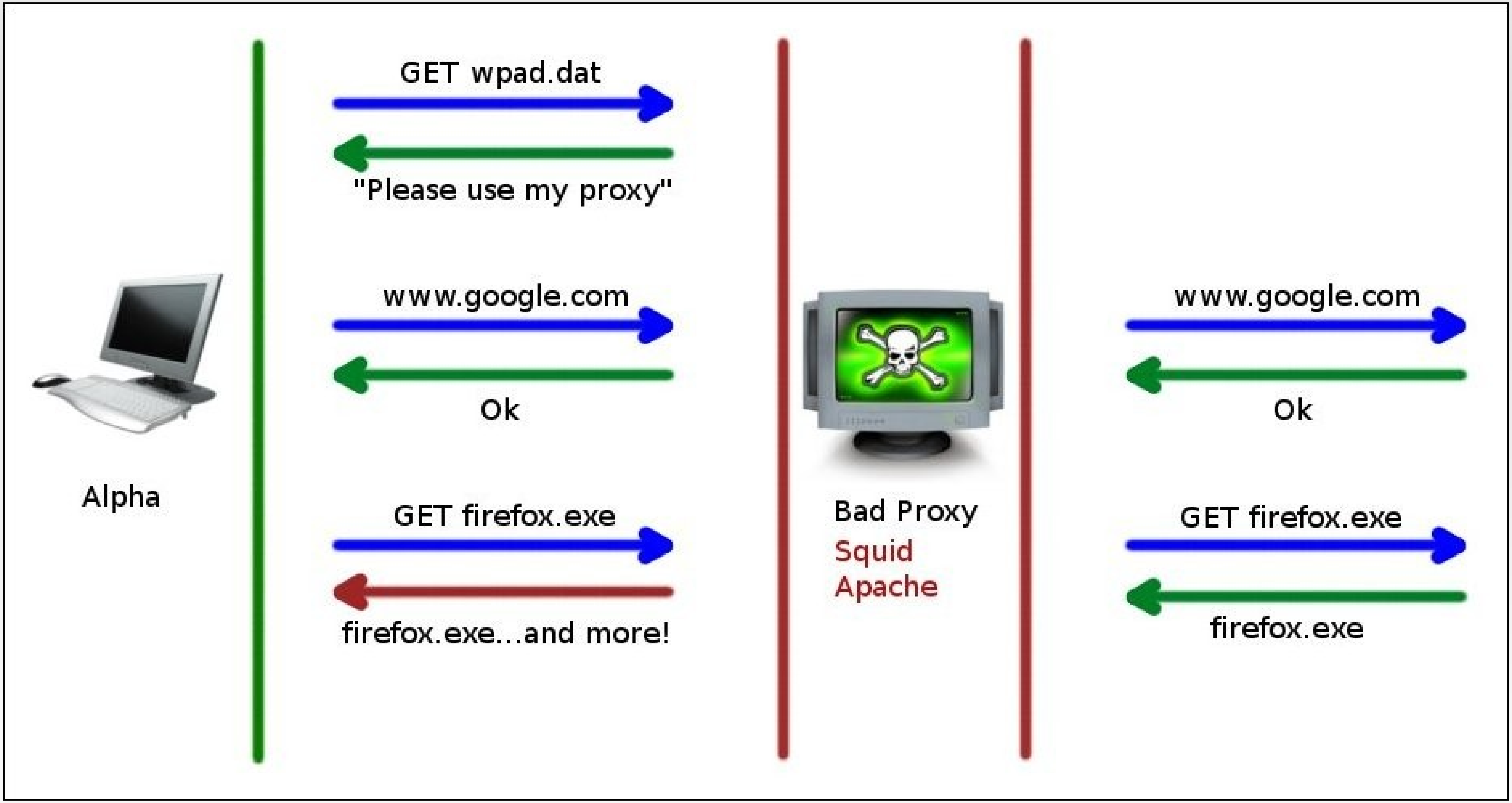
- Is this the real firefox setup.exe? NO WAY!
- Content-type: application/octet-stream
- Like this:



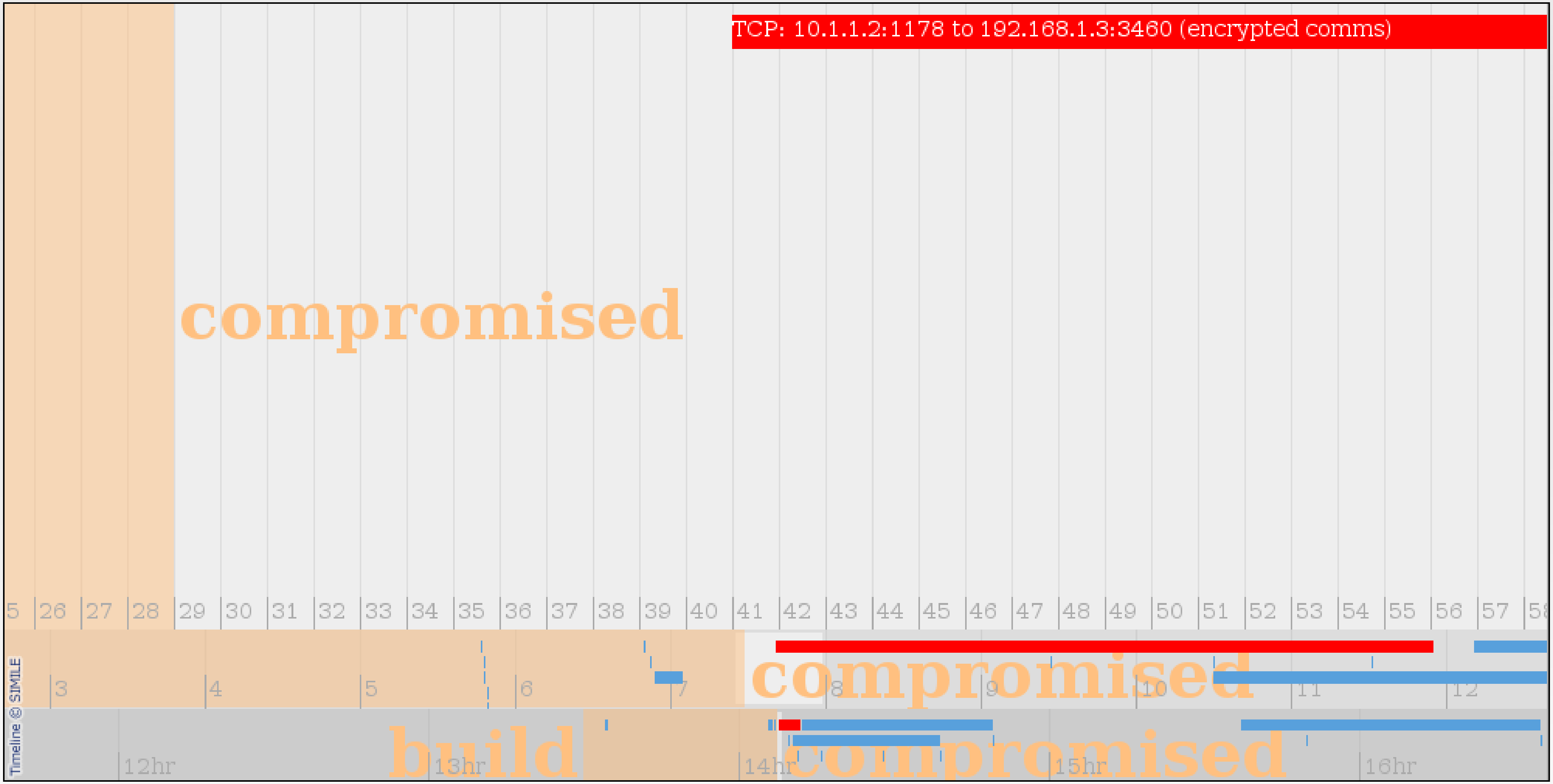
Two executables

Legitimate executable the
user requested.
e.g. the real firefox setup.exe

# 84d p0rxy


GET wpad.dat
"Please use my proxy"
www.google.com
Ok
Alpha
GET firefox.exe
firefox.exe...and more!
Bad Proxy
Squid
Apache
www.google.com
Ok
GET firefox.exe
firefox.exe

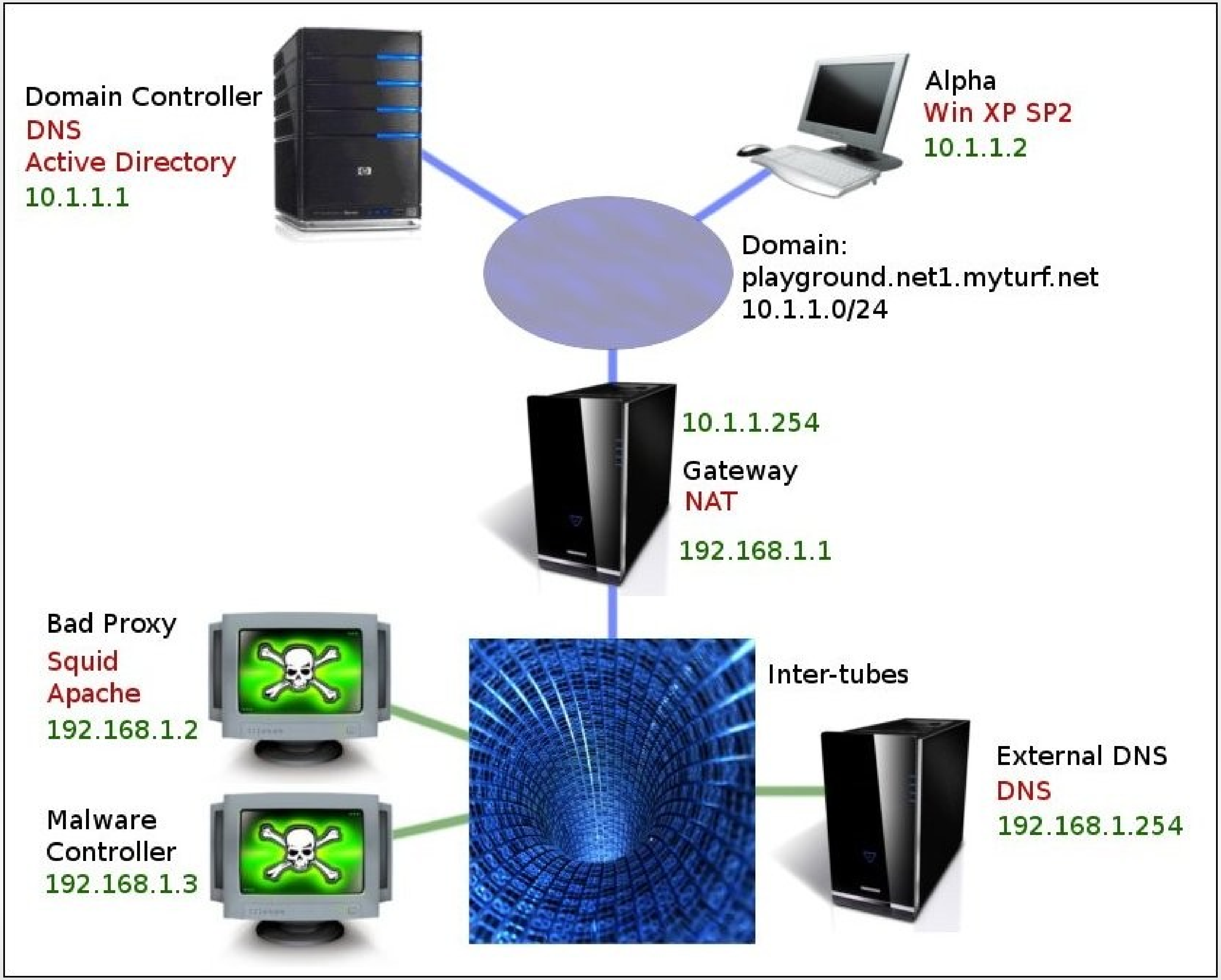
# Timeline: encrypted comms to malware controller



TCP: 10.1.1.2:1178 to 192.168.1.3:3460 (encrypted comms)

# The attack network

# The attack network



# Analysis

- Our priorities:
  1) **Cause of compromise**
  2) Extent of compromise
  3) Malware functionality & identity

# Analysis

- Our priorities:
  1) **Cause of compromise – wpad + malicious firefox**
  2) Extent of compromise
  3) Malware functionality & identity

# Analysis: disk

# Analysis: disk

- Disk tools we considered:
  - Suite: sleuthkit + autopsy
  - Utilities: many
- Tasks: Antivirus scan, MAC time analysis, browser history, event logs, registry, file carving

# Analysis: disk

- Our disk tools of choice:
  - Suite: pyFLAG
  - Utilities: clamav, mork.pl, sleuthkit (fls, mactime, dls), scalpel, md5sum, strings, file

# Analysis: disk

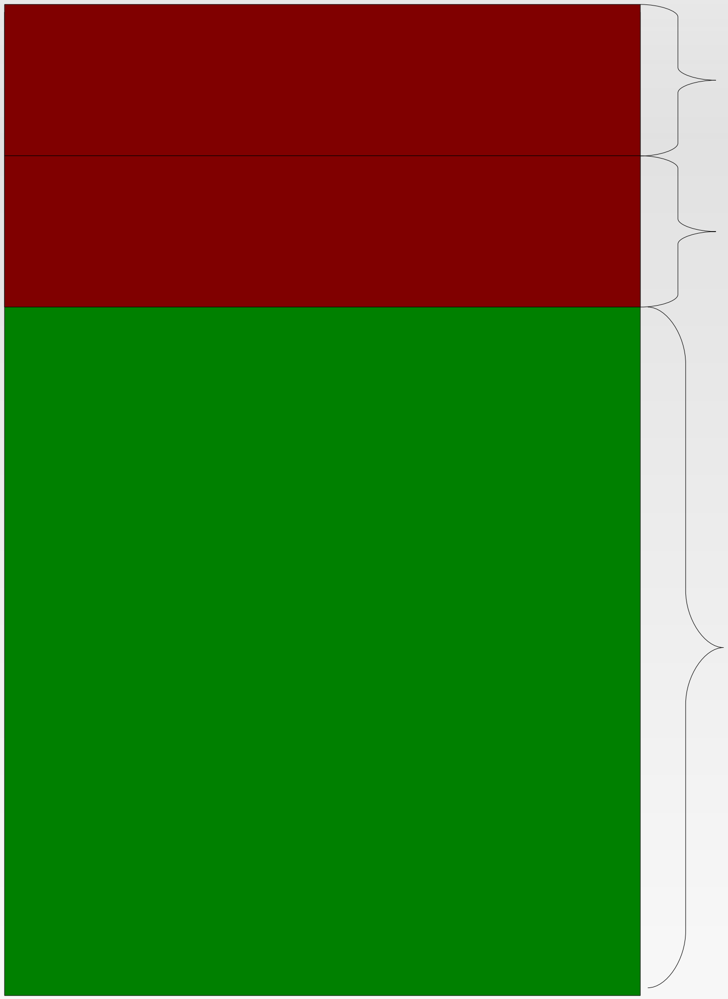
- Antivirus scan using clamav
  - Scheduled to update & scan using cron
  - Log file can be easily grep'd
  - Results can be scripted to extract infected files
- AV can be hit or miss due to variants
- Infected file: 36 (Trojan.Small-2497)
- VirusTOTAL: Backdoor.Poison variant ?

# Analysis: disk

- md5sum identified unique viruses
  - inst.exe
  - inst2.exe == MS Indexer.exe == live.exe
- Afick hash database identified these same files
- strings of each executable matched executables in firefox setup.exe

# Analysis: disk

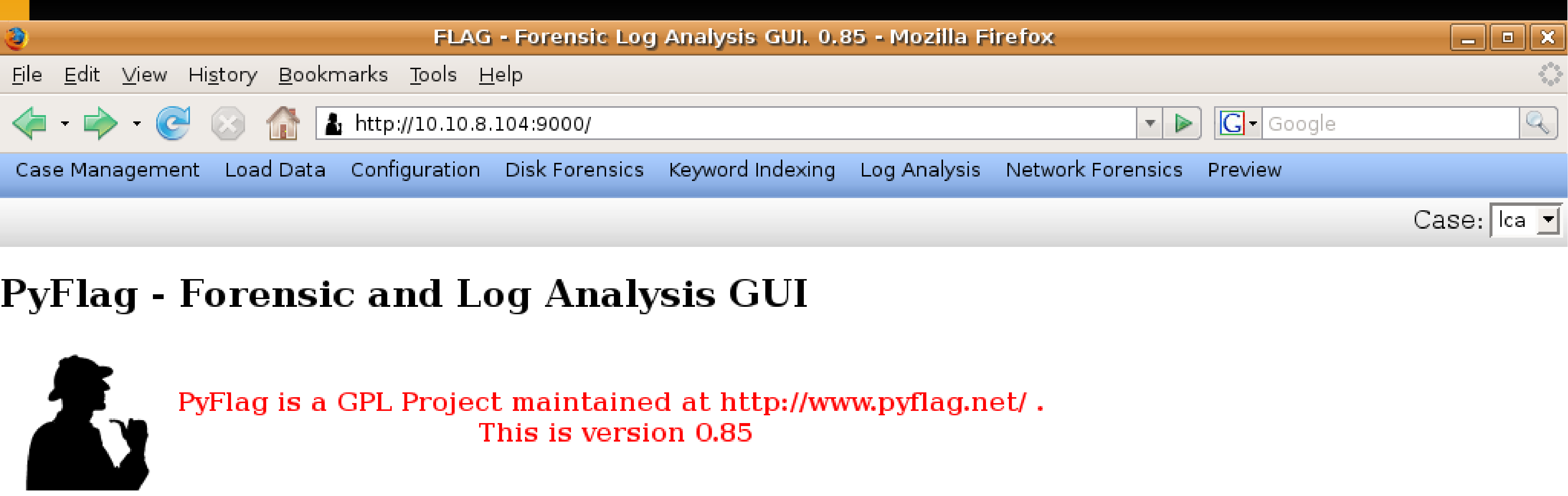
Firefox setup.exe



inst.exe

inst2.exe/MS Indexer.exe/live.exe

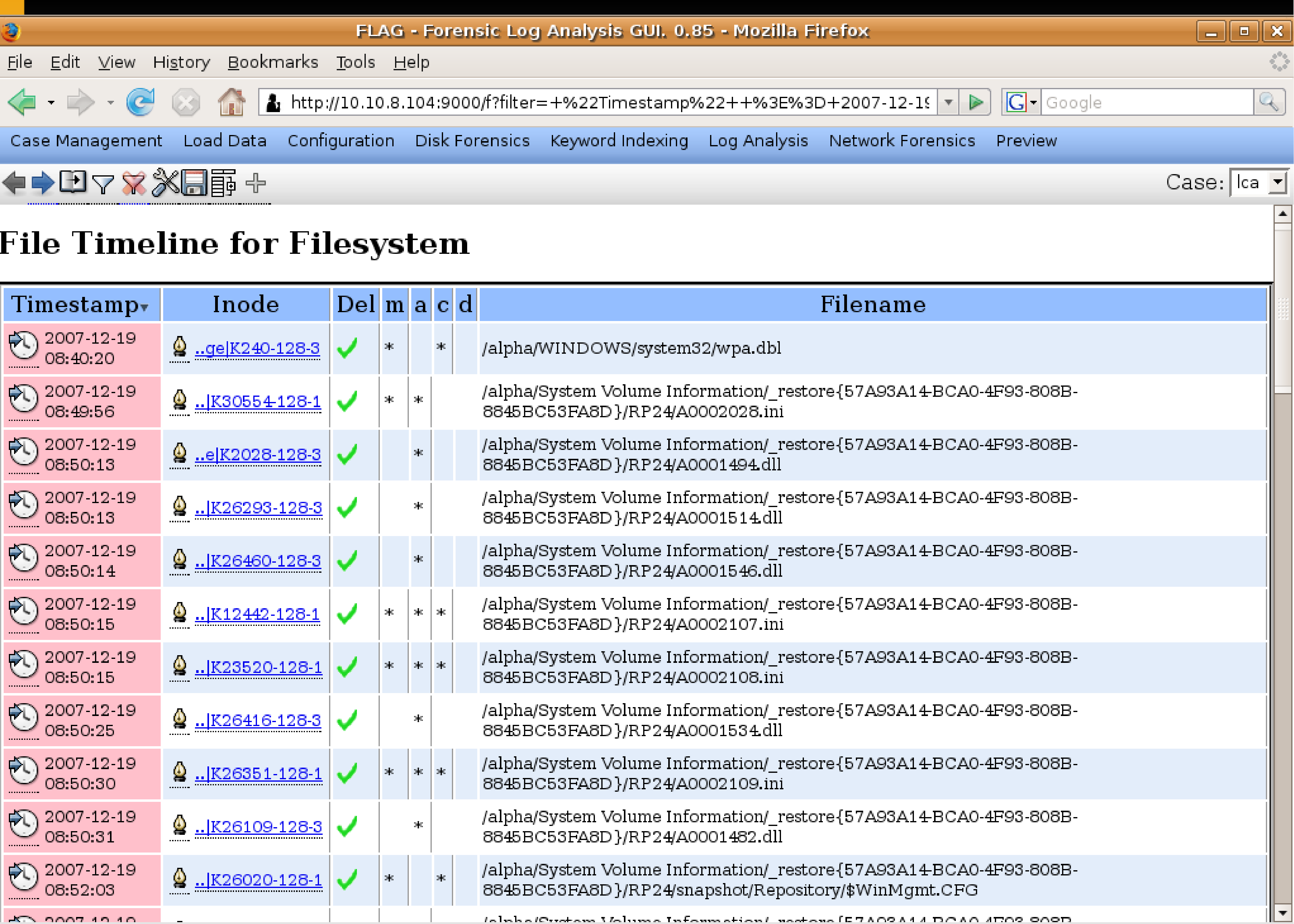
Legitimate executable the
user requested.
e.g. the real firefox setup.exe


FLAG - Forensic Log Analysis GUI. 0.85 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://10.10.8.104:9000/
Google
Case Management Load Data Configuration Disk Forensics Keyword Indexing Log Analysis Network Forensics Preview
Case: lca

PyFlag - Forensic and Log Analysis GUI

PyFlag is a GPL Project maintained at http://www.pyflag.net/ .
This is version 0.85

- MAC times (files and registry hives)
- Event log
- IE browser cache



# File Timeline for Filesystem

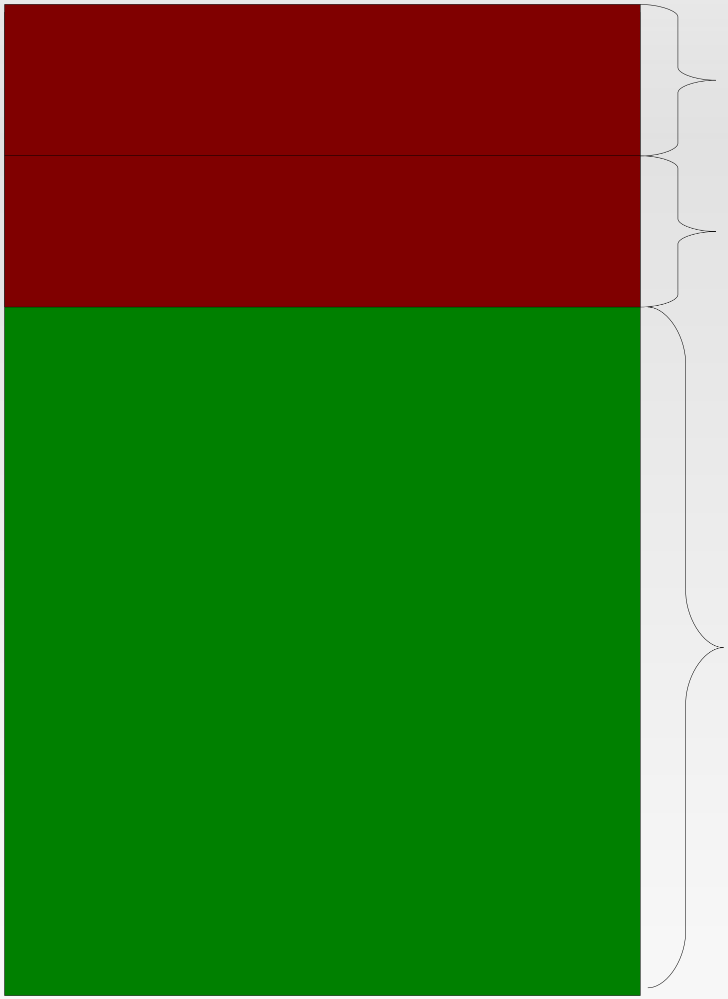
| Timestamp | Inode | Del | m | a | c | d | Filename |
|---|---|---|---|---|---|---|---|
| 2007-12-19 08:40:20 | ..ge\|K240-128-3 | ✓ | * |  | * |  | /alpha/WINDOWS/system32/wpa.dbl |
| 2007-12-19 08:49:56 | ..\|K30554-128-1 | ✓ | * | * |  |  | /alpha/System Volume Information/_restore{57A93A14-BCA0-4F93-808B-8845BC53FA8D}/RP24/A0002028.ini |
| 2007-12-19 08:50:13 | ..e\|K2028-128-3 | ✓ |  | * |  |  | /alpha/System Volume Information/_restore{57A93A14-BCA0-4F93-808B-8845BC53FA8D}/RP24/A0001494.dll |
| 2007-12-19 08:50:13 | ..\|K26293-128-3 | ✓ |  | * |  |  | /alpha/System Volume Information/_restore{57A93A14-BCA0-4F93-808B-8845BC53FA8D}/RP24/A0001514.dll |
| 2007-12-19 08:50:14 | ..\|K26460-128-3 | ✓ |  | * |  |  | /alpha/System Volume Information/_restore{57A93A14-BCA0-4F93-808B-8845BC53FA8D}/RP24/A0001546.dll |
| 2007-12-19 08:50:15 | ..\|K12442-128-1 | ✓ | * | * | * |  | /alpha/System Volume Information/_restore{57A93A14-BCA0-4F93-808B-8845BC53FA8D}/RP24/A0002107.ini |
| 2007-12-19 08:50:15 | ..\|K23520-128-1 | ✓ | * | * | * |  | /alpha/System Volume Information/_restore{57A93A14-BCA0-4F93-808B-8845BC53FA8D}/RP24/A0002108.ini |
| 2007-12-19 08:50:25 | ..\|K26416-128-3 | ✓ |  | * |  |  | /alpha/System Volume Information/_restore{57A93A14-BCA0-4F93-808B-8845BC53FA8D}/RP24/A0001534.dll |
| 2007-12-19 08:50:30 | ..\|K26351-128-1 | ✓ | * | * | * |  | /alpha/System Volume Information/_restore{57A93A14-BCA0-4F93-808B-8845BC53FA8D}/RP24/A0002109.ini |
| 2007-12-19 08:50:31 | ..\|K26109-128-3 | ✓ |  | * |  |  | /alpha/System Volume Information/_restore{57A93A14-BCA0-4F93-808B-8845BC53FA8D}/RP24/A0001482.dll |
| 2007-12-19 08:52:03 | ..\|K26020-128-1 | ✓ | * |  | * |  | /alpha/System Volume Information/_restore{57A93A14-BCA0-4F93-808B-8845BC53FA8D}/RP24/snapshot/Repository/$WinMgmt.CFG |

# Analysis: disk

- pyFLAG enabled us to:
  - Confirm initial compromise
  - Determine how the malware unpacks

# Analysis: how the malware unpacks

Firefox setup.exe

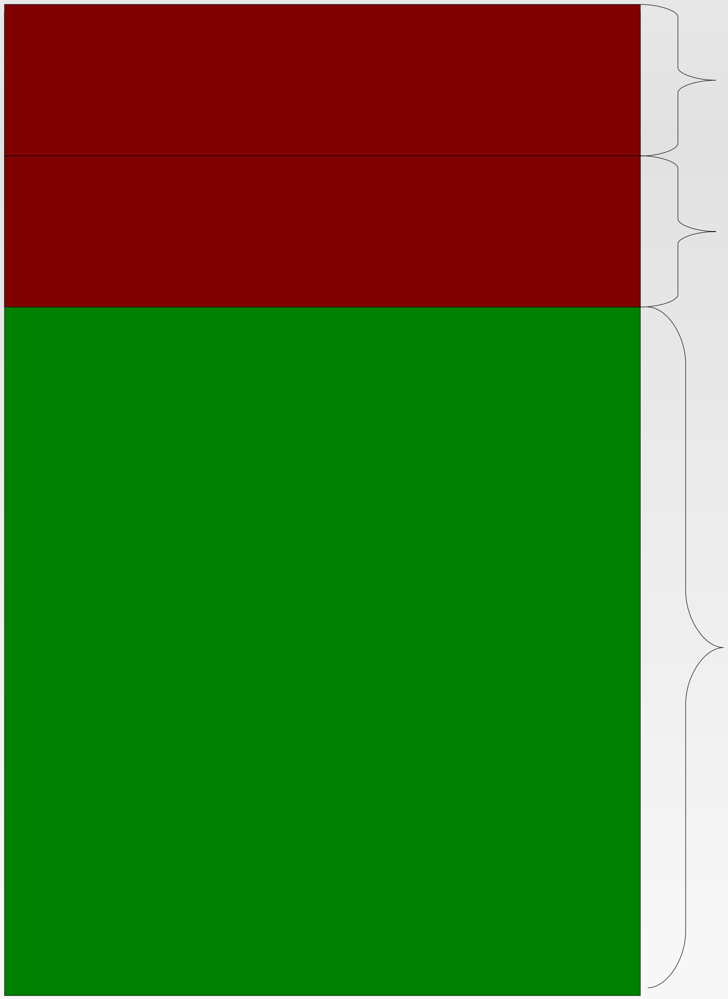


inst.exe

inst2.exe/MS Indexer.exe/live.exe

Legitimate executable the
user requested.
e.g. the real firefox setup.exe

# Analysis: how the malware unpacks



Firefox setup.exe

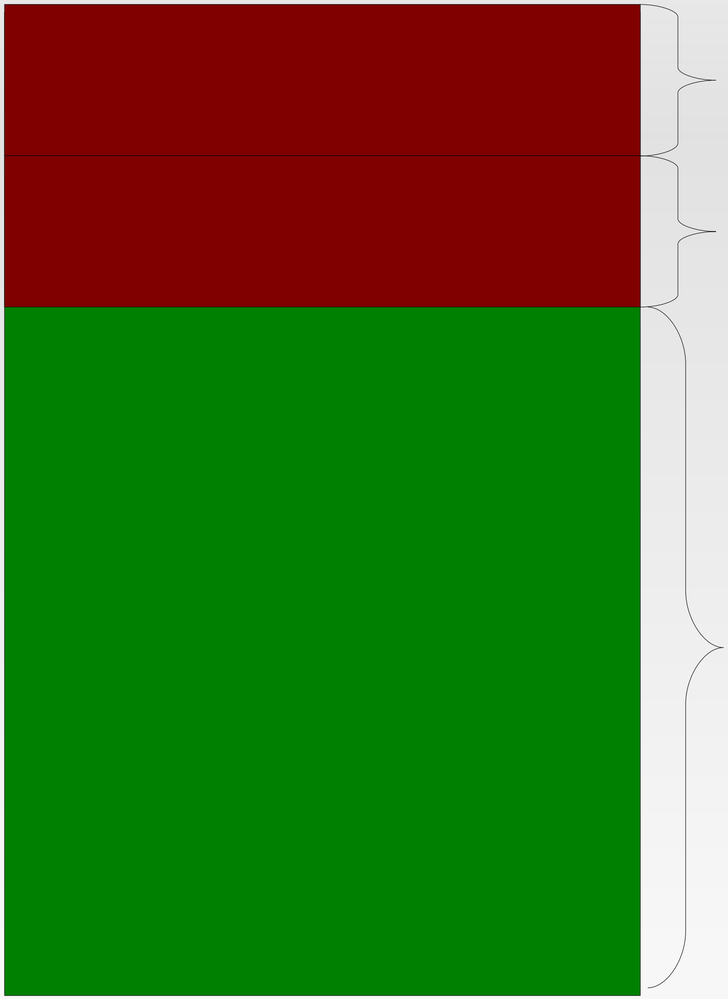
Unpacker

inst2.exe/MS Indexer.exe/live.exe

Legitimate executable the
user requested.
e.g. the real firefox setup.exe

# Analysis: how the malware unpacks

Firefox setup.exe



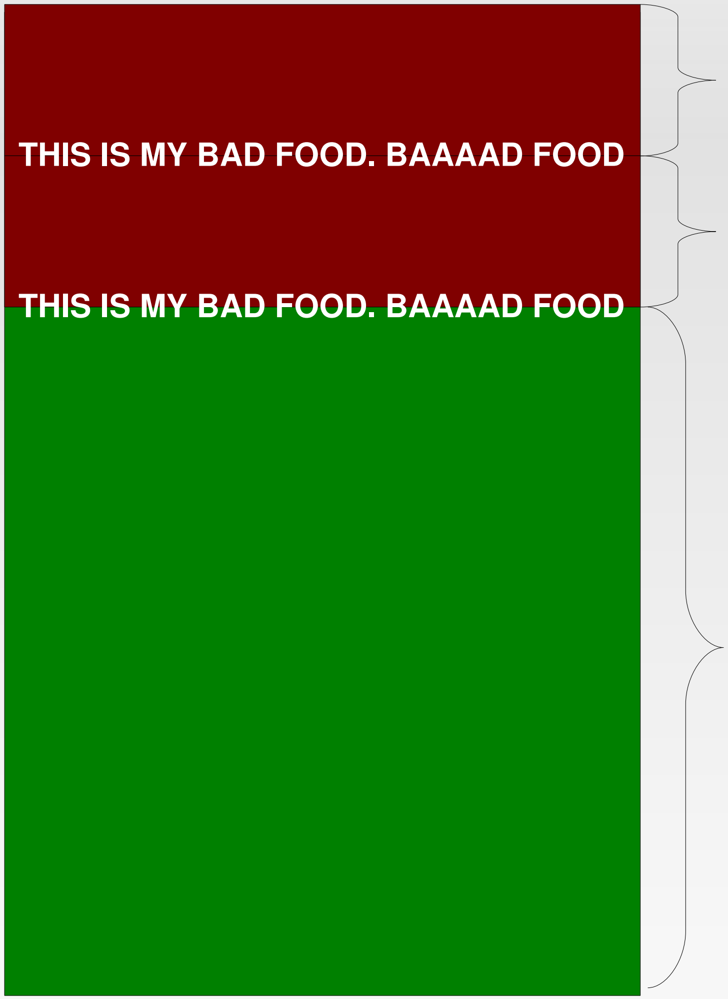
Unpacker

Trojan/malware

Legitimate executable the user requested.
e.g. the real firefox setup.exe

# Analysis: how the malware unpacks

Firefox setup.exe

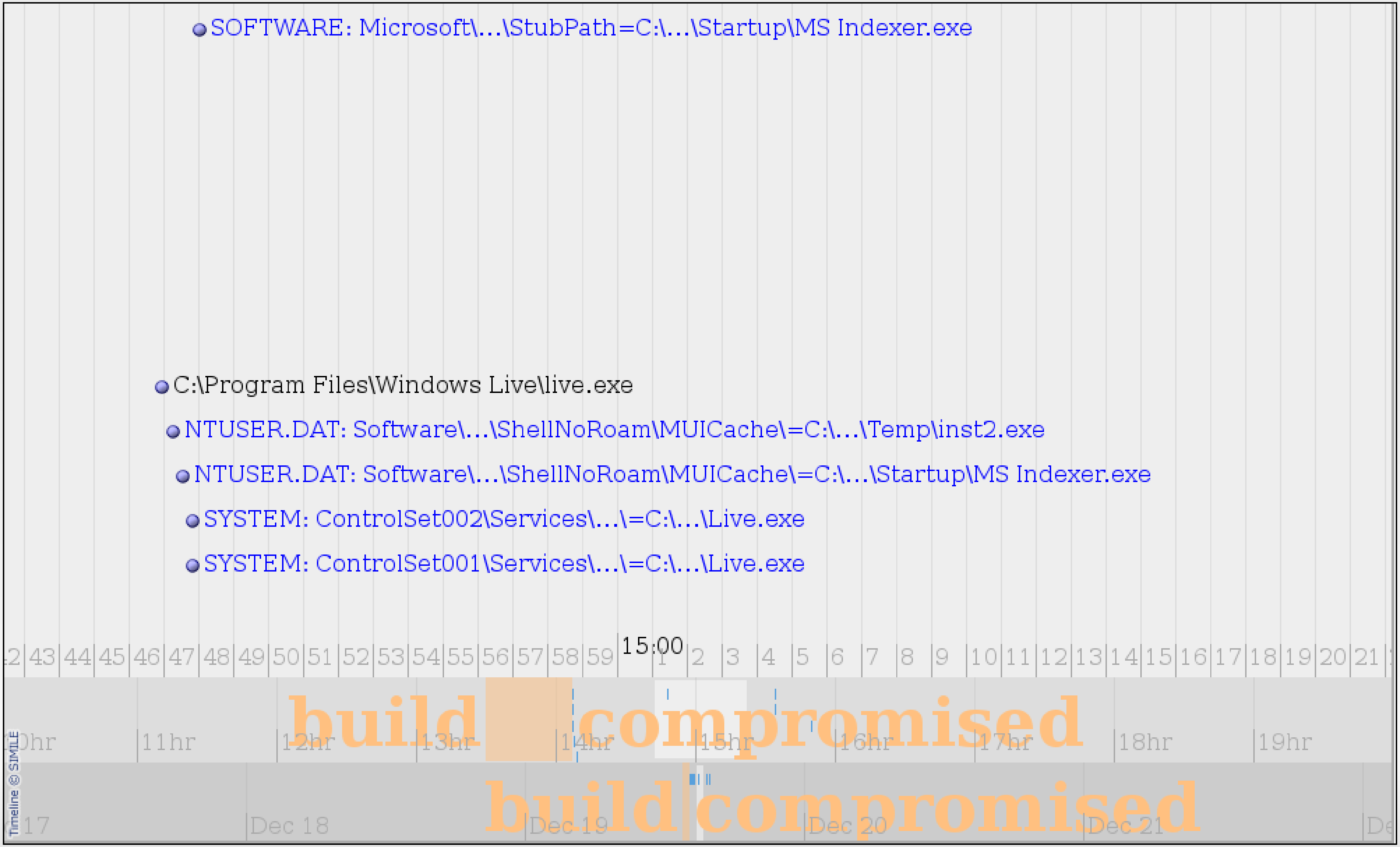

THIS IS MY BAD FOOD. BAAAAD FOOD
THIS IS MY BAD FOOD. BAAAAD FOOD

Unpacker

Trojan/malware

Legitimate executable the user requested.
e.g. the real firefox setup.exe

# Timeline: persistence



SOFTWARE: Microsoft\...\StubPath=C:\...\Startup\MS Indexer.exe

C:\Program Files\Windows Live\live.exe

NTUSER.DAT: Software\...\ShellNoRoam\MUICache\=C:\...\Temp\inst2.exe

NTUSER.DAT: Software\...\ShellNoRoam\MUICache\=C:\...\Startup\MS Indexer.exe

SYSTEM: ControlSet002\Services\...\=C:\...\Live.exe

SYSTEM: ControlSet001\Services\...\=C:\...\Live.exe

# Analysis

- Our priorities:

1) Cause of compromise – wpad + malicious firefox
2) **Extent of compromise**
   -
   -
3) Malware functionality & identity

# Analysis

- Our priorities:

1) Cause of compromise – wpad + malicious firefox
2) **Extent of compromise**
   - **Malware: inst2.exe**
   - **Methods of persistence: reg keys, start up**
3) Malware functionality & identity

# Analysis

- Our priorities:

1) Cause of compromise – wpad + malicious firefox

2) Extent of compromise
   - Malware: inst2.exe
   - Methods of persistence: reg keys, start up

3) **Malware functionality** & identity
   -

# Analysis

- Our priorities:
  1) Cause of compromise – wpad + malicious firefox
  2) Extent of compromise
     - Malware: inst2.exe
     - Methods of persistence: reg keys, start up
  3) **Malware functionality** & identity
     - **Functionality: keylogging, password hashes, file upload, encrypted comms**

# Analysis: memory

# Analysis: memory

- Memory tools we considered:
  - PTFinder
  - PoolTools
  - Windows IR/CF tools
- Our memory tool of choice: volatility

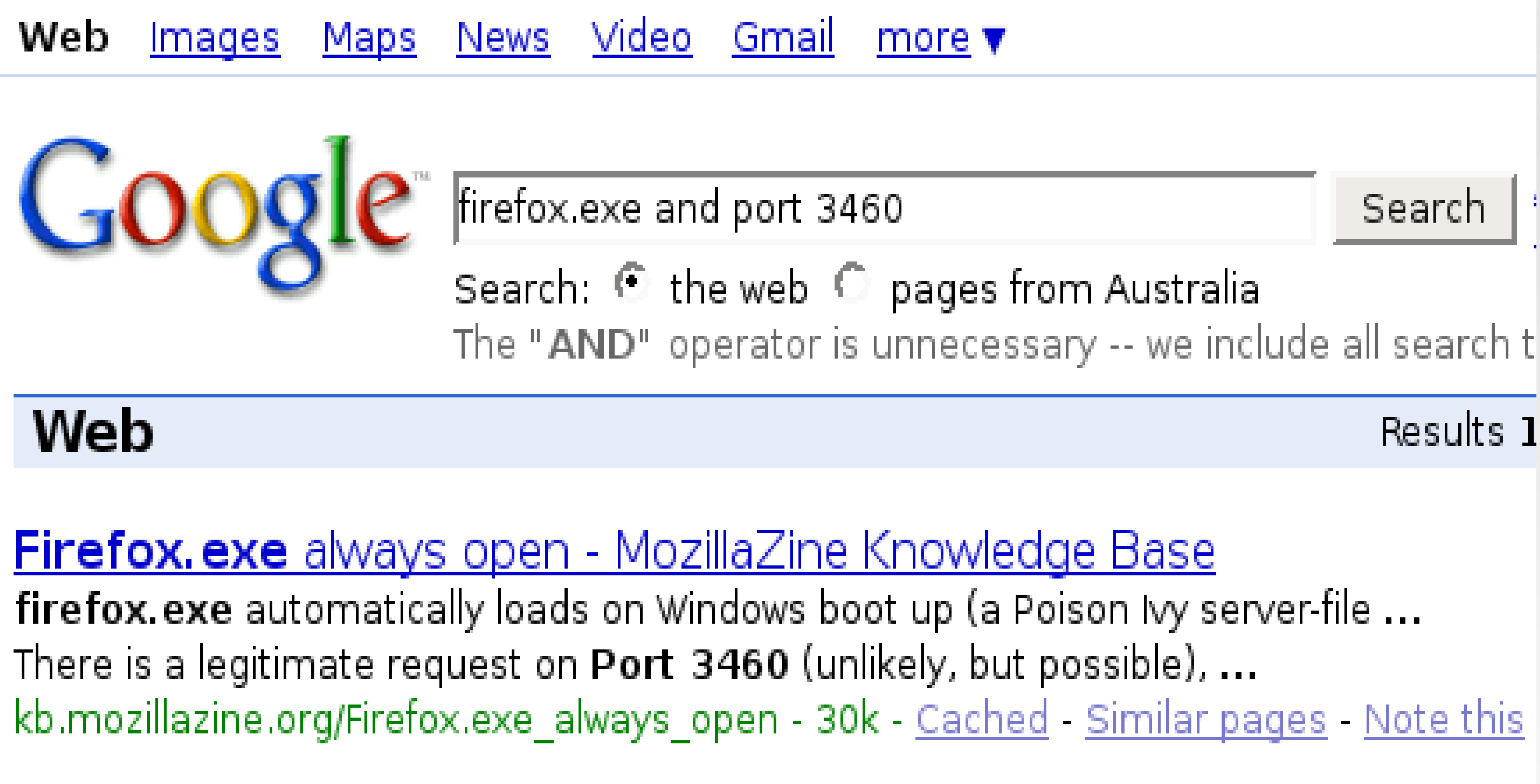
# DEMO:

## Memory analysis using volatility

# Analysis: memory

- pslist: firefox.exe (1812)
- firefox.exe not running when memory acquired!
- connections: firefox.exe (1812) to 192.168.1.3:3460
- dlllist: parameters to firefox.exe, non-standard?

# Analysis: memory



firefox.exe and port 3460

Search: ● the web ○ pages from Australia

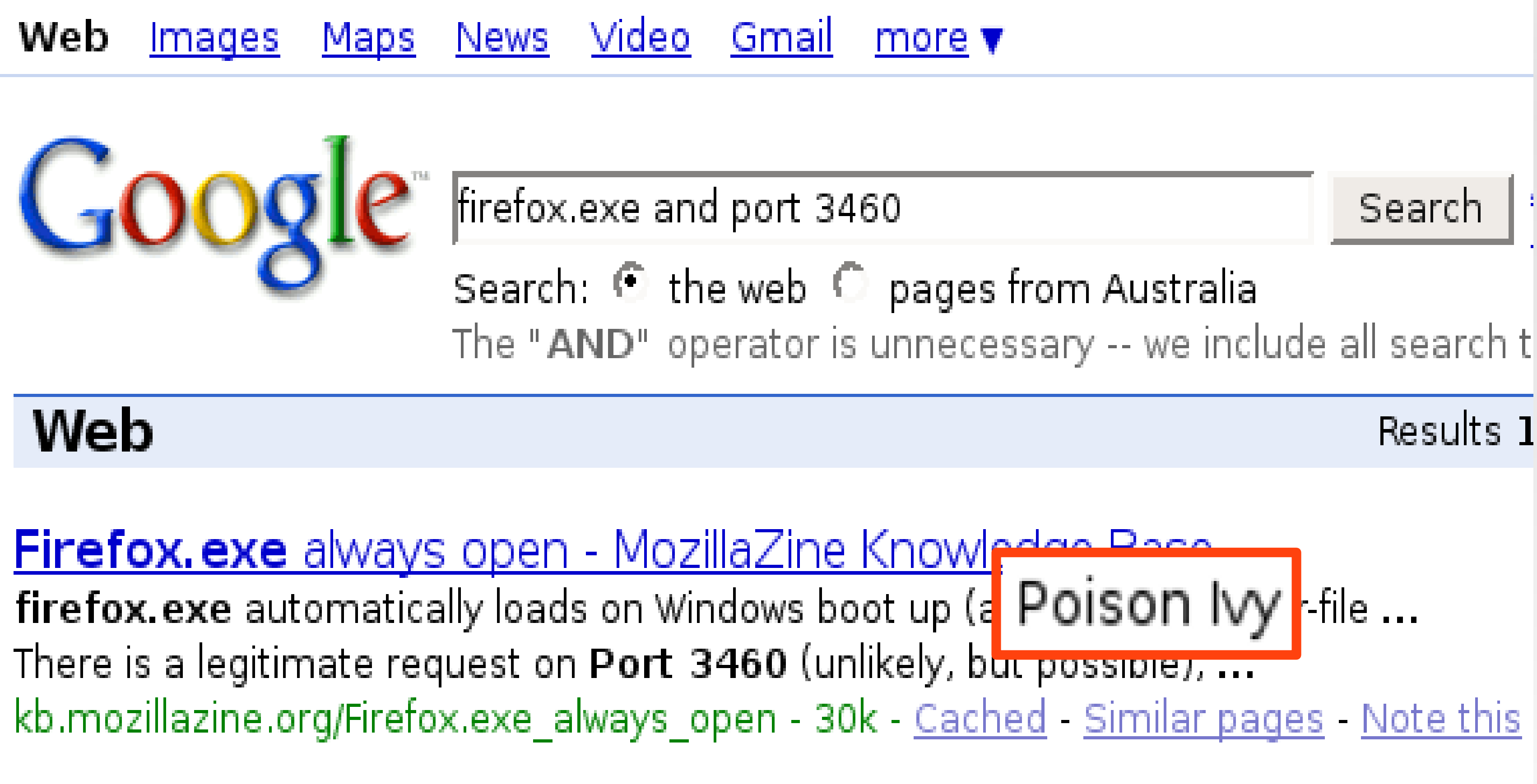
The "**AND**" operator is unnecessary -- we include all search t

**Web** Results **1**

**Firefox.exe** always open - MozillaZine Knowledge Base

**firefox.exe** automatically loads on Windows boot up (a Poison Ivy server-file **...**
There is a legitimate request on **Port 3460** (unlikely, but possible), **...**
kb.mozillazine.org/Firefox.exe_always_open - 30k - Cached - Similar pages - Note this

# Analysis: memory



firefox.exe and port 3460

Search: ● the web ○ pages from Australia

The "**AND**" operator is unnecessary -- we include all search t

**Web** Results 1

**Firefox.exe** always open - MozillaZine Knowl

**firefox.exe** automatically loads on Windows boot up (a -file ...

There is a legitimate request on **Port 3460** (unlikely, but possible), ...

kb.mozillazine.org/Firefox.exe_always_open - 30k - Cached - Similar pages - Note this

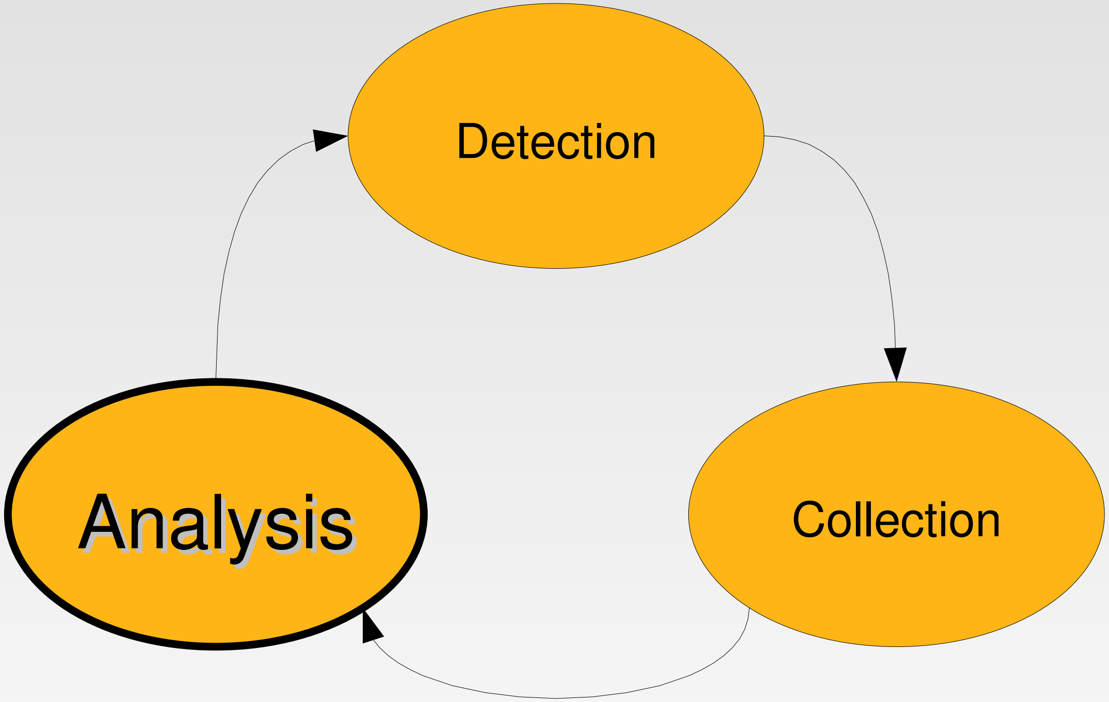
Poison Ivy

# Analysis

- Our priorities:
  1) Cause of compromise – wpad + malicious firefox
  2) Extent of compromise
     - Malware: inst2.exe
     - Methods of persistence: reg keys, start up
  3) **Malware** functionality & **identity**
     - Functionality: keylogging, password hashes, file upload, encrypted comms
     - **Identity: PoisonIvy**

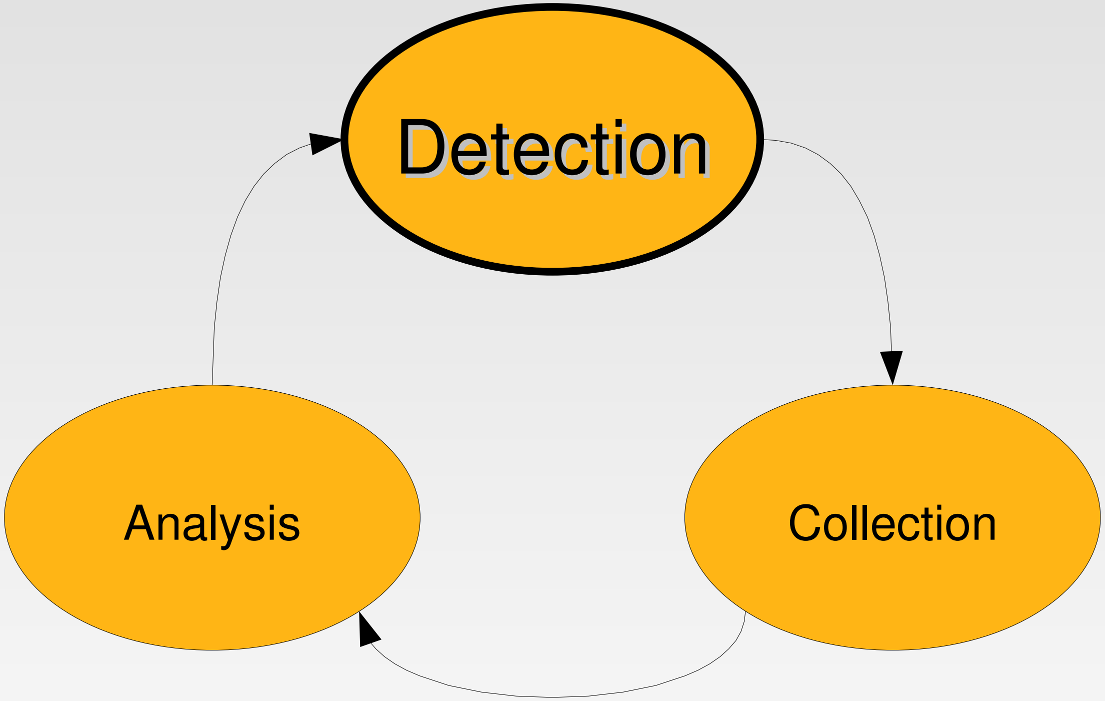
# Investigation

- The incident
- **IR life cycle**
  - Detection
  - Collection
  - **Analysis**



# Investigation

- The incident
- **IR life cycle**
  - **Detection**
  - Collection
  - Analysis



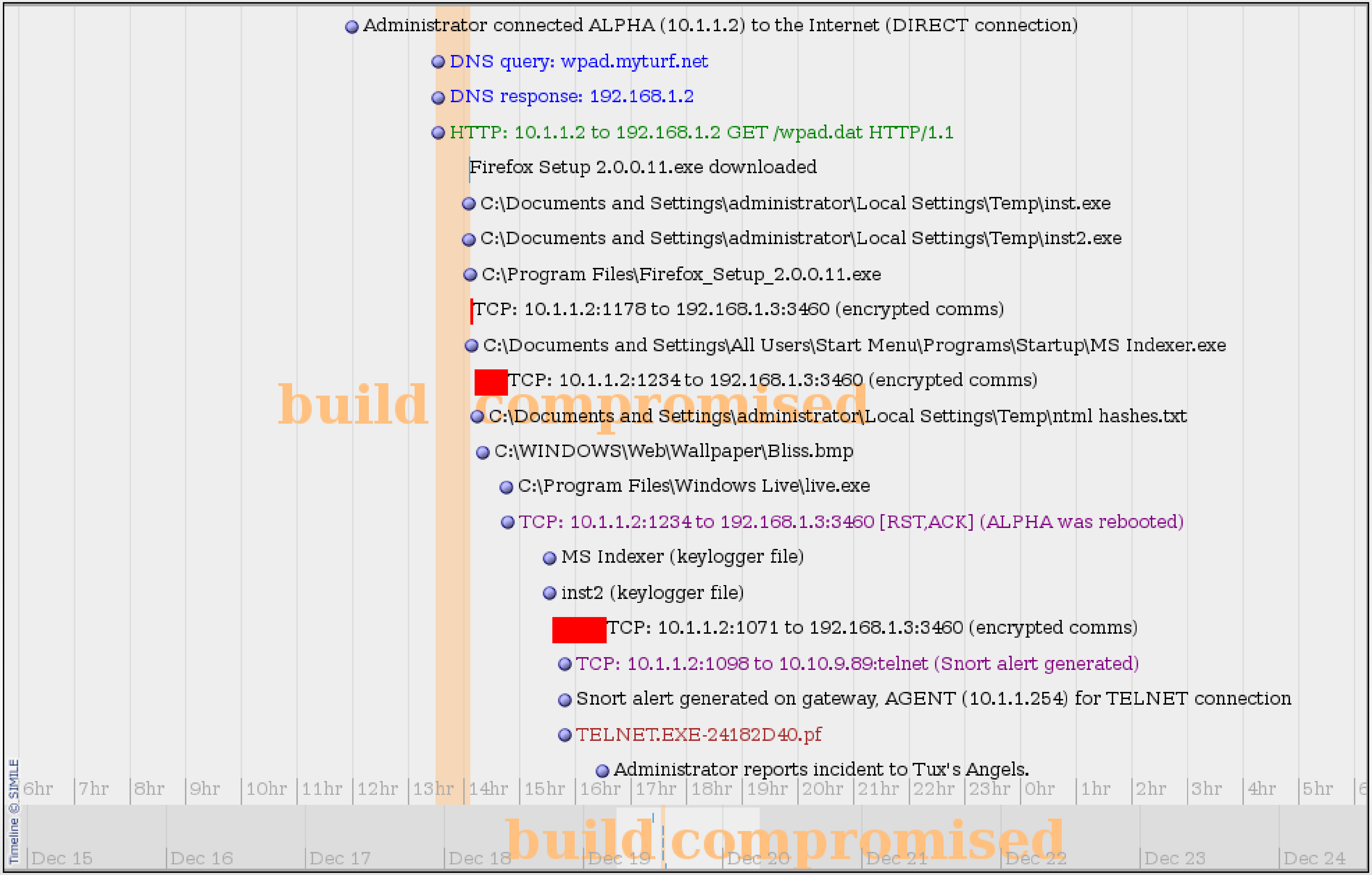
# Agenda

- Incident response
- Linux + FOSS
- **Investigation**
- Conclusion

# Agenda

- Incident response
- Linux + FOSS
- Investigation
- **Conclusion**

# Final Timeline: Investigation SOLVED!



Administrator connected ALPHA (10.1.1.2) to the Internet (DIRECT connection)

DNS query: wpad.myturf.net

DNS response: 192.168.1.2

HTTP: 10.1.1.2 to 192.168.1.2 GET /wpad.dat HTTP/1.1

Firefox Setup 2.0.0.11.exe downloaded

C:\Documents and Settings\administrator\Local Settings\Temp\inst.exe

C:\Documents and Settings\administrator\Local Settings\Temp\inst2.exe

C:\Program Files\Firefox_Setup_2.0.0.11.exe

TCP: 10.1.1.2:1178 to 192.168.1.3:3460 (encrypted comms)

C:\Documents and Settings\All Users\Start Menu\Programs\Startup\MS Indexer.exe

TCP: 10.1.1.2:1234 to 192.168.1.3:3460 (encrypted comms)

C:\Documents and Settings\administrator\Local Settings\Temp\ntml hashes.txt

C:\WINDOWS\Web\Wallpaper\Bliss.bmp

C:\Program Files\Windows Live\live.exe

TCP: 10.1.1.2:1234 to 192.168.1.3:3460 [RST,ACK] (ALPHA was rebooted)

MS Indexer (keylogger file)

inst2 (keylogger file)

TCP: 10.1.1.2:1071 to 192.168.1.3:3460 (encrypted comms)

TCP: 10.1.1.2:1098 to 10.10.9.89:telnet (Snort alert generated)

Snort alert generated on gateway, AGENT (10.1.1.254) for TELNET connection

TELNET.EXE-24182D40.pf

Administrator reports incident to Tux's Angels.

# Ok, so what now?

- Block outbound comms
- Prevent further compromise
- Reimage infected machines
- Ensure no mechanism for persistence
- Assess damage

# Linux + FOSS

- Tool wrap up
  - Detection: swatch/snort/dumpcap/BASE
  - Collection: dcfldd/FAUdd/tcpdump
  - Analysis: wireshark/pyFLAG (and others)/volatility
- How you can use these tools, even if you're not in an IR team?

# Thanks...

- Our bad guy: Eddie Cornejo
- LCA

# Thank you. Any questions?

- References (images):
  - Alpha http://www.co.orange.nc.us/library/libsvcs/computer.gif
  - DC http://www.mikeschinkel.com/blog/content/binary/windows-home-server-from-hp.png
  - Gateway http://blogs.zdnet.com/microsoft/images/Medion%20Home%20Server.jpg
  - Internet http://www.goemerchant.com/images/gateway.jpg
  - Badguy http://www.daleypws.com/images/bad_pc.jpg
  - Dragons http://www.forcounsel.com/products/4104.jpg