What is HACIENDA?

- Data reconnaissance tool developed by the CITD team in JTRIG
- Port Scans entire countries
  - Uses nmap as port scanning tool
  - Uses GEOFUSION for IP Geolocation
  - Randomly scans every IP identified for that country

[redacted]

Countries

- Completed full scans of 27 countries including
  - [redacted]
- Completed partial scans of 5 additional countries

[redacted]

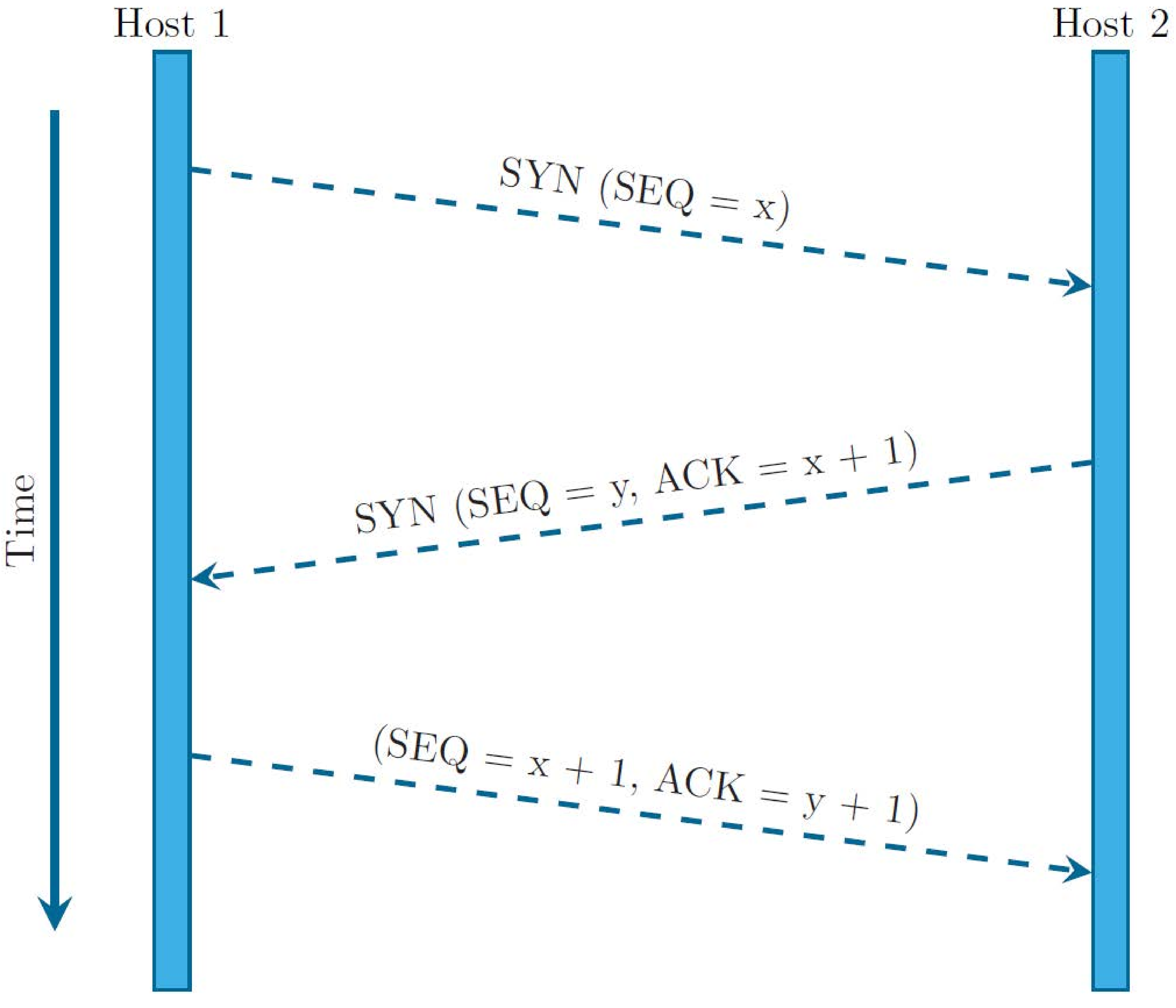
Tasking & Access

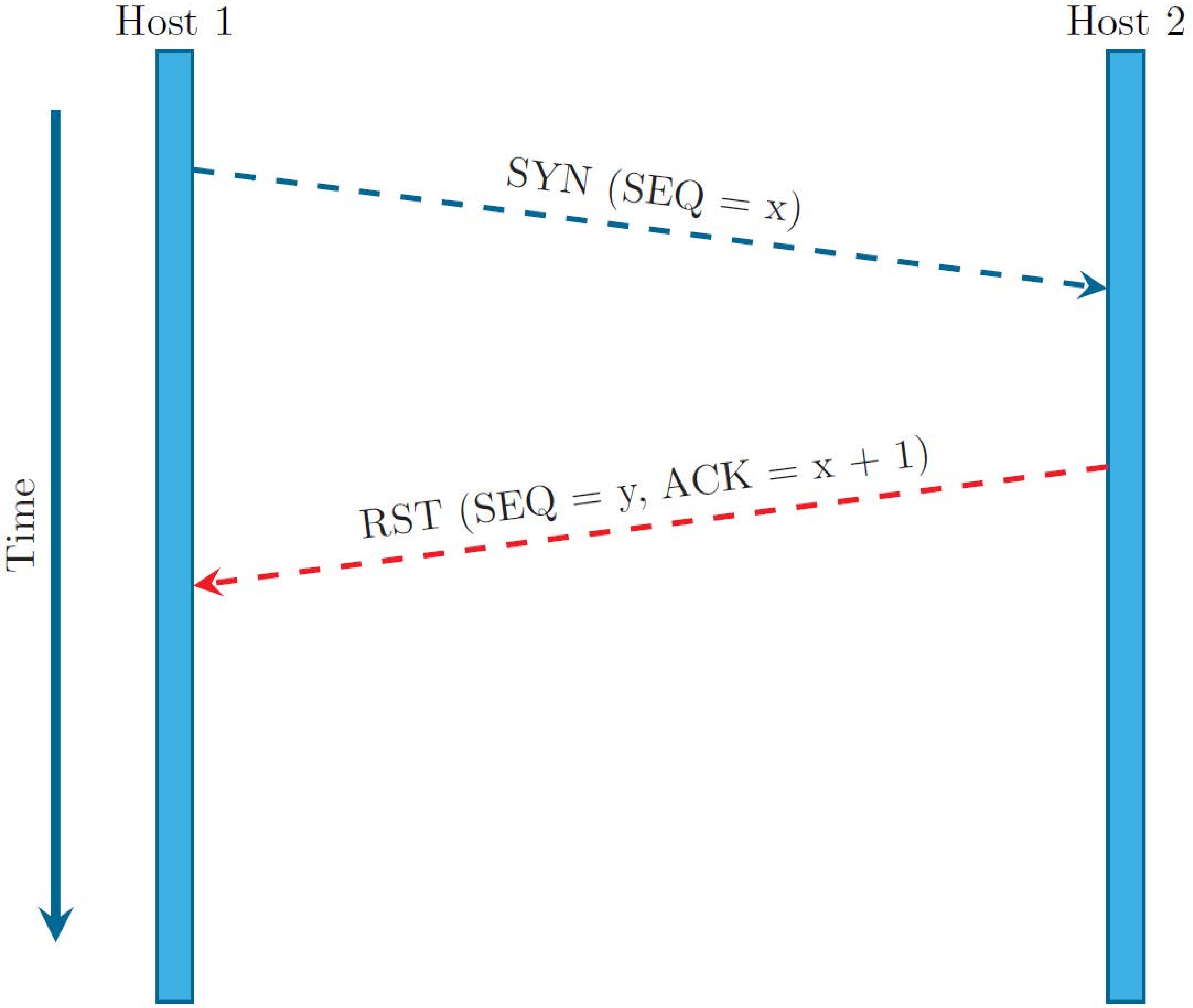
- To task HACIENDA with a Country or Subnet
  - [redacted]@gchq.gov.uk)
  - CITD alias ([redacted]@gchq.gov.uk)

- Access to the Data
  - At GCHQ, request a GLOBAL SURGE account from [redacted]@gchq.gov.uk)
  - At CSEC, contact [redacted]
  - At NSA, contact [redacted]
  - At DSD, contact [redacted]

Ports

- Pulls back hostname, banners, application names and port status
- Gathers additional information for…
  - 21 (ftp): directory listing
  - 80 (http): content of main page
  - 443 (https): content of main page
  - 111 (rpc): results of rpcinfo


Host 1
Host 2
Time
SYN (SEQ = x)
SYN (SEQ = y, ACK = x + 1)
(SEQ = x + 1, ACK = y + 1)


Host 1
Host 2
SYN (SEQ = x)
RST (SEQ = y, ACK = x + 1)
Time

The Results…

- All stored in JTRIG's internal database
- Available in GLOBAL SURGE
  - NAC's Network Knowledge Base Prototype
- Transferred by MAILORDER to
  - CSEC
  - DSD
  - NSA NTOC

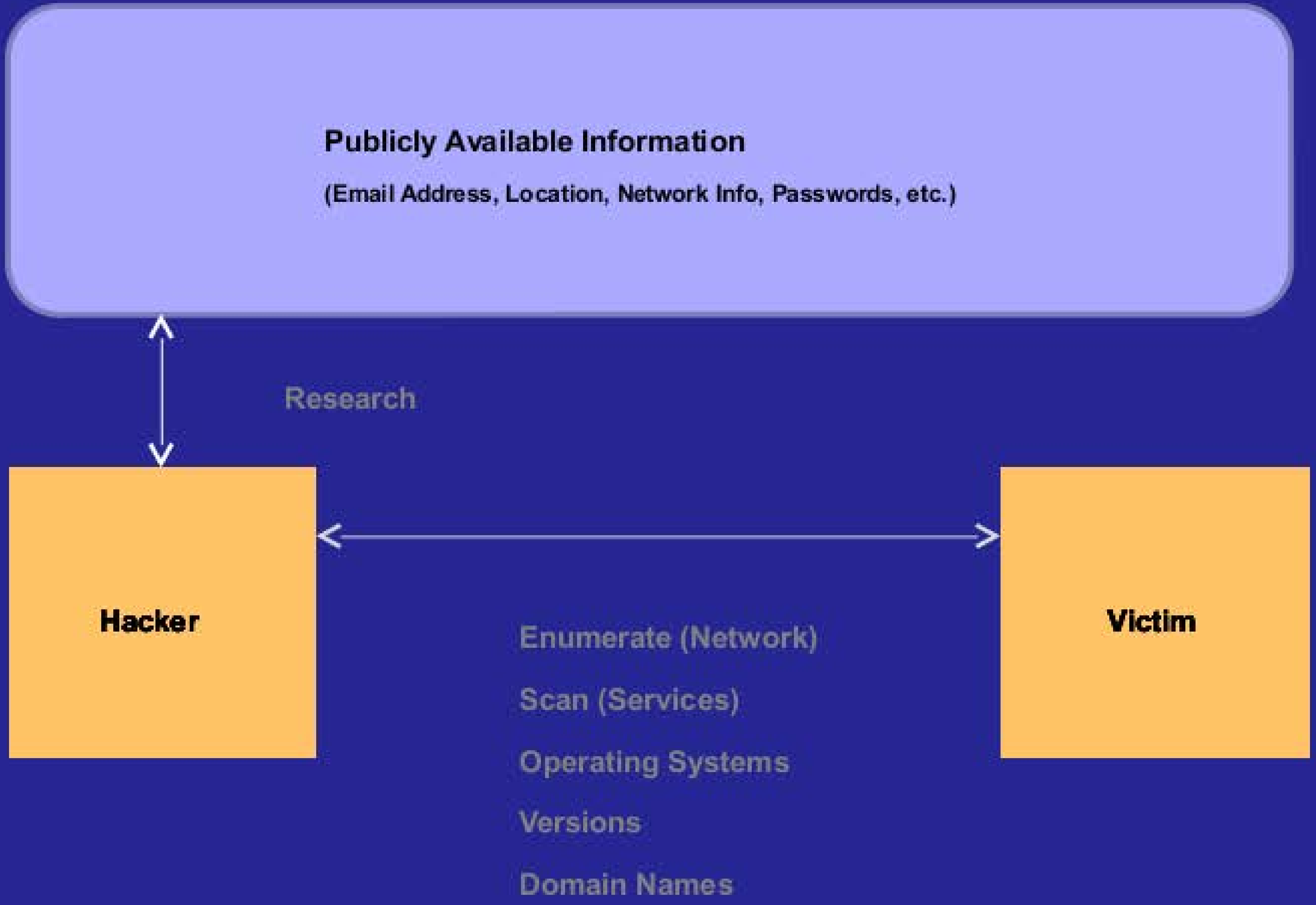
How is it used?

- CNE
  - ORB Detection
  - Vulnerability Assessments
- SD
  - Network Analysis
  - Target Discovery

The Hacking Process

1. (**R**)econnaissance
2. (**I**)nfection
3. (**C**)ommand And Control
4. (**E**)xfiltration

Reconnaissance



Publicly Available Information

(Email Address, Location, Network Info, Passwords, etc.)

Research

Hacker

Victim

Enumerate (Network)

Scan (Services)

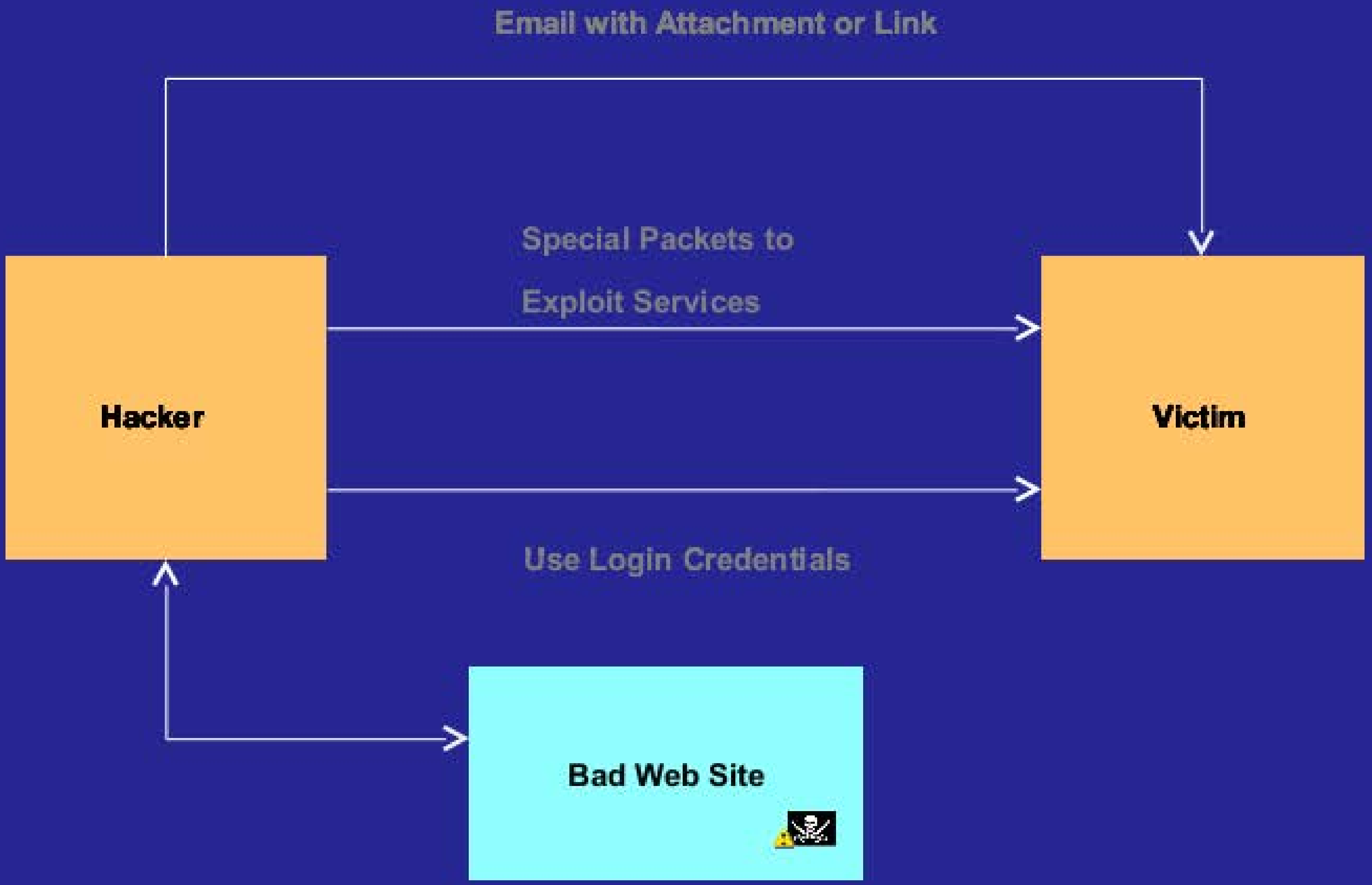
Operating Systems

Versions

Domain Names

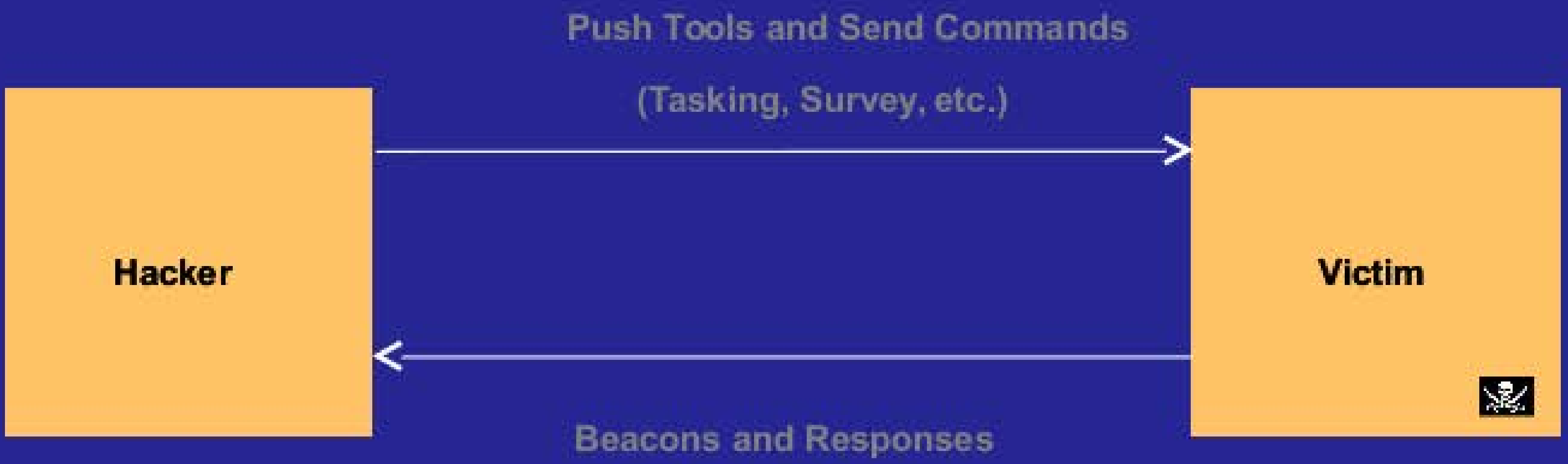
Reconnaissance Infection Command and Control Exfiltration

Infection



Reconnaissance **Infection** Command and Control Exfiltration

Command and Control

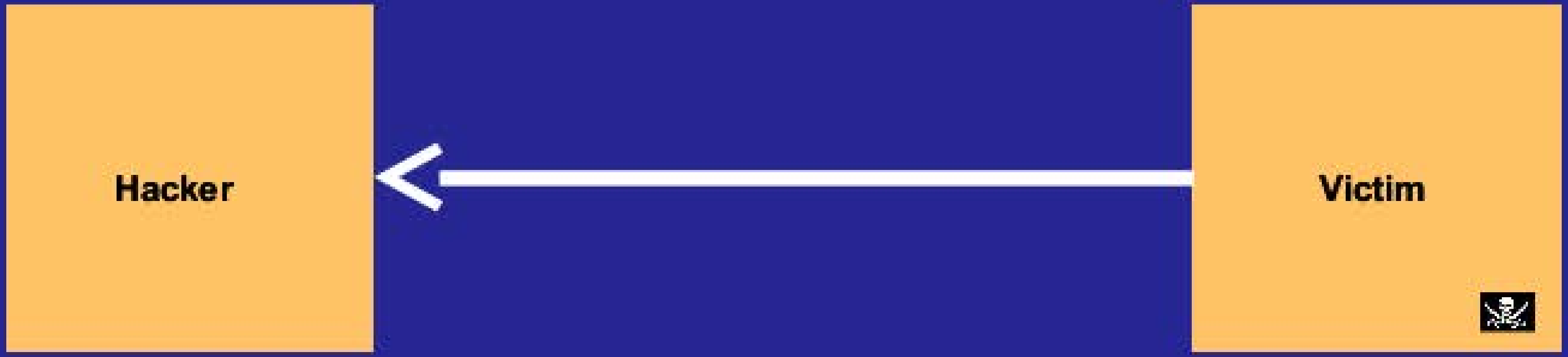


Reconnaissance Infection **Command and Control** Exfiltration

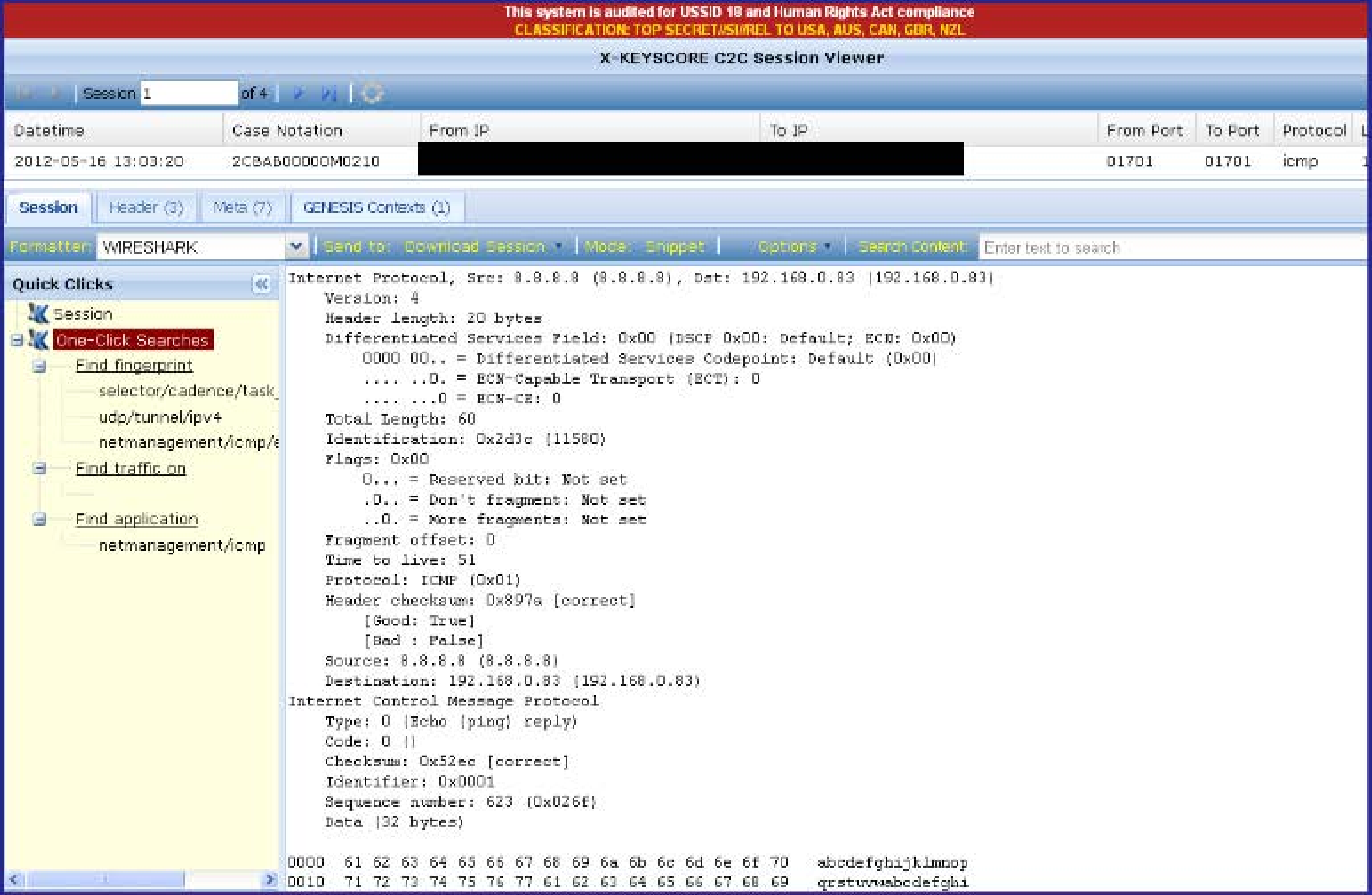
Exfiltration

Exfil using known and custom protocols

(Known: HTTP, SMTP, ICMP, FTP, etc)



Reconnaissance



This system is audited for USSID 18 and Human Rights Act compliance
CLASSIFICATION: TOP SECRET//SI//REL TO USA, AUS, CAN, GBR, NZL

X-KEYSCORE C2C Session Viewer

Datetime	Case Notation	From IP	To IP	From Port	To Port	Protocol
2012-05-16 13:03:20	2CBAB0000OM0210	[redacted]	[redacted]	01701	01701	icmp

Formatter: WIRESHARK

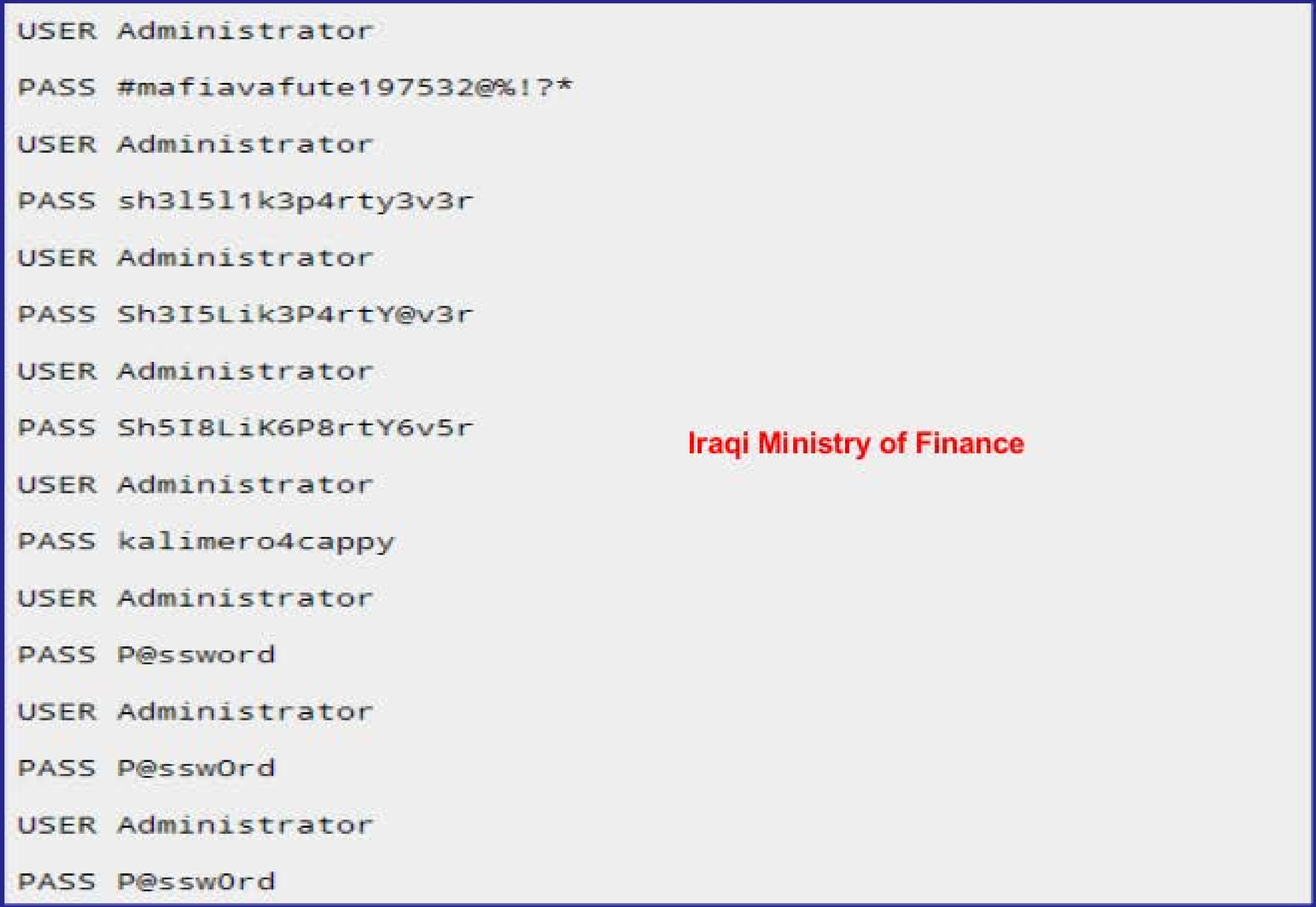
Mode: Snippet

```
Internet Protocol, Src: 8.8.8.8 (8.8.8.8), Dst: 192.168.0.83 (192.168.0.83)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 60
    Identification: 0x2d3c (11580)
    Flags: 0x00
        0... = Reserved bit: Not set
        .0.. = Don't fragment: Not set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 51
    Protocol: ICMP (0x01)
    Header checksum: 0x897a [correct]
        [Good: True]
        [Bad : False]
    Source: 8.8.8.8 (8.8.8.8)
    Destination: 192.168.0.83 (192.168.0.83)
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0 ()
    Checksum: 0x52ec [correct]
    Identifier: 0x0001
    Sequence number: 623 (0x026f)
    Data (32 bytes)

0000  61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70   abcdefghijklmnop
0010  71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69   qrstuvwabcdefghi
```

Reconnaissance Infection Command and Control Exfiltration

Password Guessing

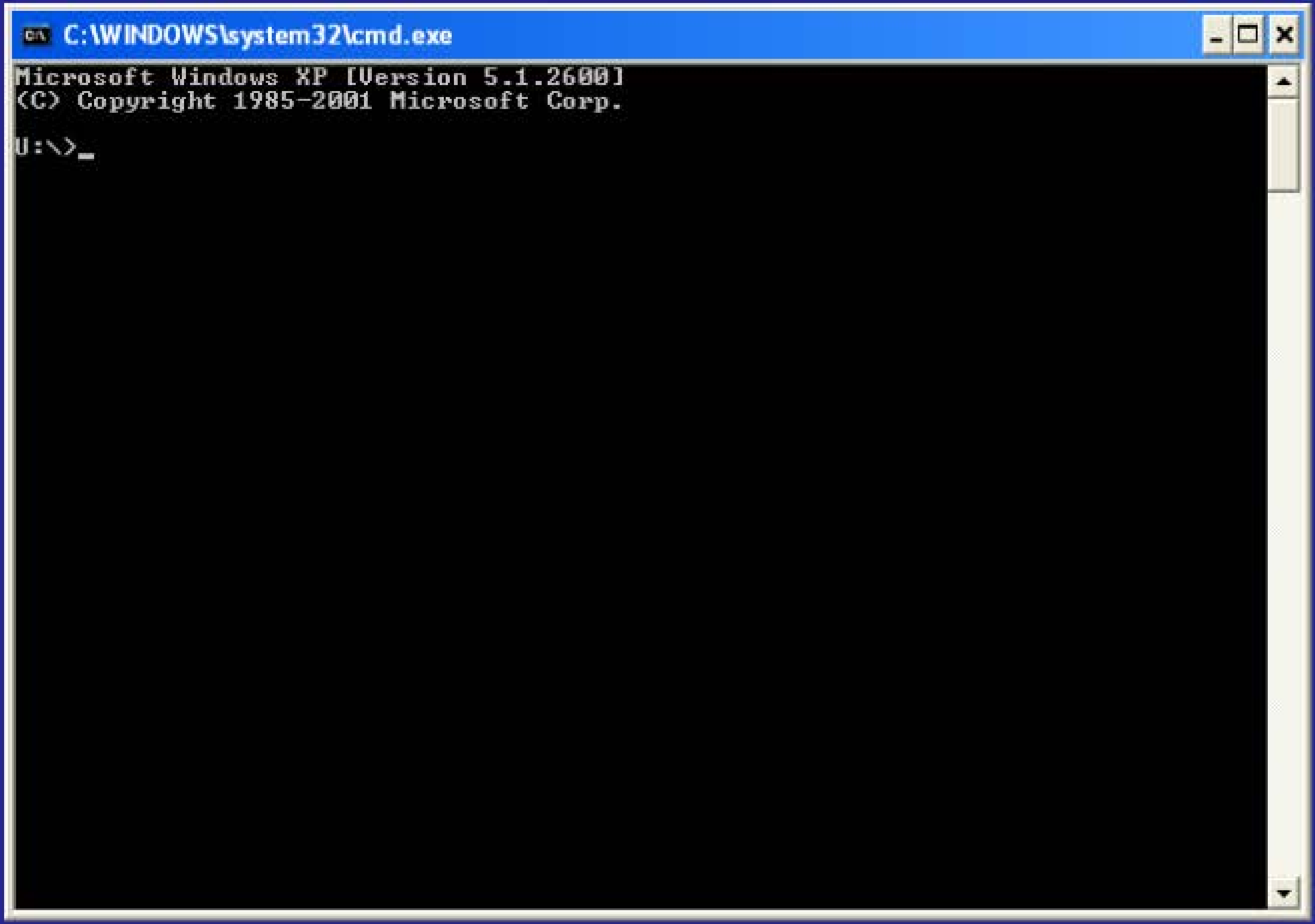


```
USER Administrator
PASS #mafiavafute197532@%!?*
USER Administrator
PASS sh3l5l1k3p4rty3v3r
USER Administrator
PASS Sh3I5Lik3P4rtY@v3r
USER Administrator
PASS Sh5I8LiK6P8rtY6v5r
USER Administrator
PASS kalimero4cappy
USER Administrator
PASS P@ssword
USER Administrator
PASS P@ssw0rd
USER Administrator
PASS P@ssw0rd
```

Iraqi Ministry of Finance

Reconnaissance Infection Command and Control Exfiltration

Windows cmd.exe



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

U:\>_
```

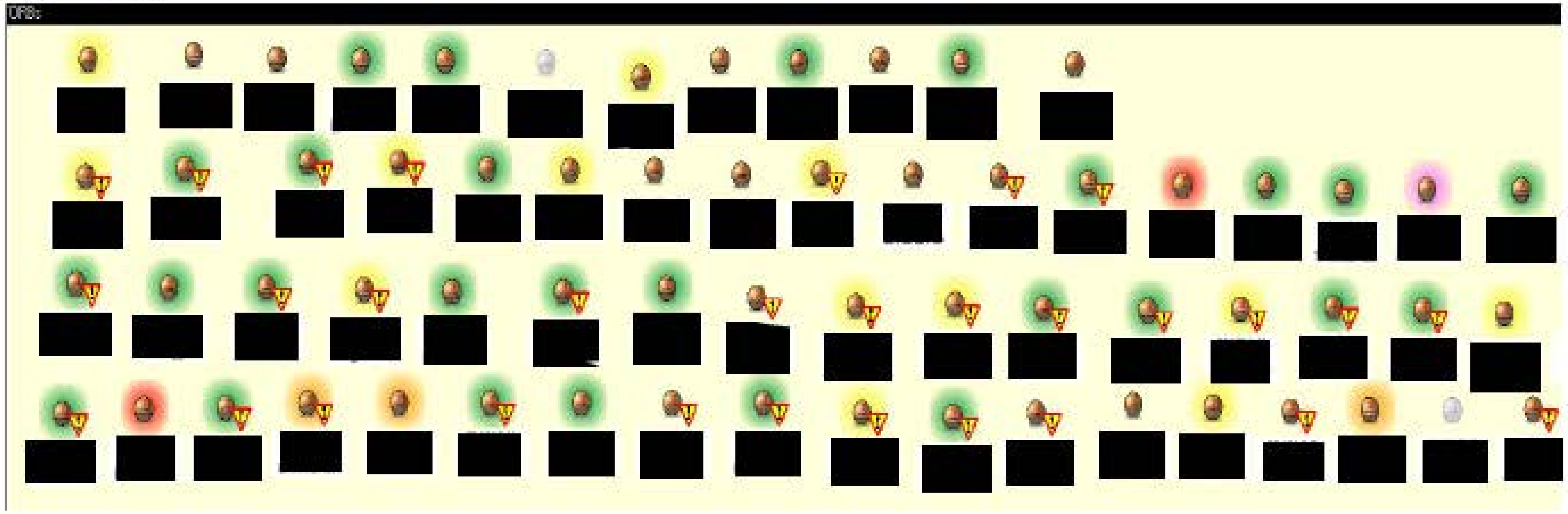
Reconnaissance Infection Command and Control Exfiltration

Presentation Outline

- LANDMARK – automated tradecraft to further expand CNE covert infrastructure
- [redacted]

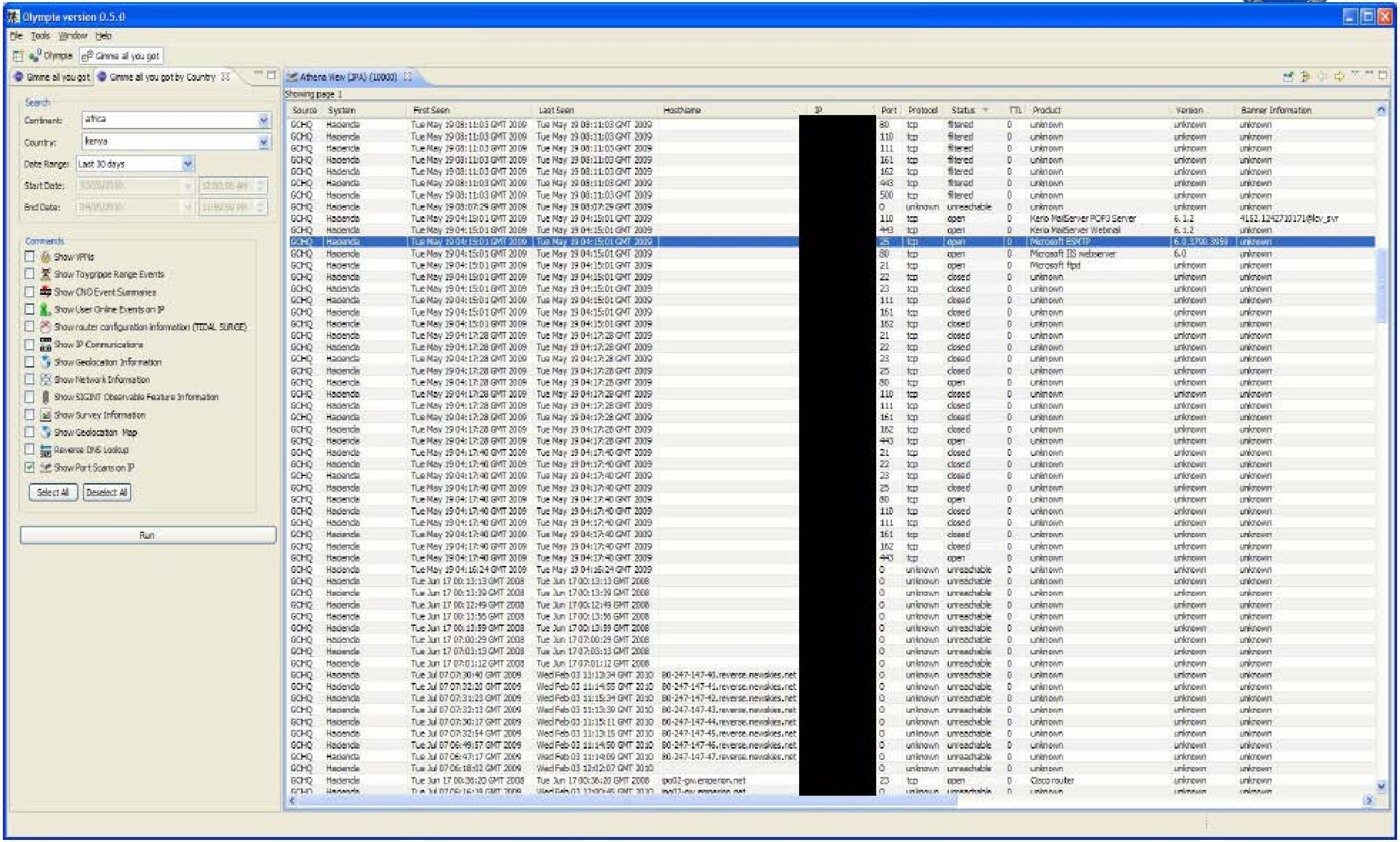
LANDMARK

- CSEC's Operational Relay Box (ORB) covert infrastructure used to provide an additional level of non-attribution; subsequently used for exploits and exfiltration
- 2-3 times/year, 1 day focused effort to acquire as many new ORBs as possible in as many non 5-Eyes countries as possible


ORBs:
[redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted]
[redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted]
[redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted]
[redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted]

LANDMARK – the recent past….

- February 2010
- Operation encompassing the whole of LONGRUN solely using OLYMPIA (CSEC's network knowledge engine with automated tradecraft)
- 8 teams of 3 network exploitation analysts busy for 5-8 hours
- A list of 3000+ potential ORBs



Search

Continent: africa

Country: kenya

Date Range: Last 30 days

Start Date: 03/20/2010 12:00:00 AM

End Date: 04/20/2010 11:59:59 PM

Commands

- ☐ Show VPNs
- ☐ Show Toygripe Range Events
- ☐ Show CNO Event Summaries
- ☐ Show User Online Events on IP
- ☐ Show router configuration information (TIDAL SURGE)
- ☐ Show IP Communications
- ☐ Show Geolocation Information
- ☐ Show Network Information
- ☐ Show SIGINT Observable Feature Information
- ☐ Show Survey Information
- ☐ Show Geolocation Map
- ☐ Reverse DNS Lookup
- ☑ Show Port Scans on IP

Showing page 1

Source	System	First Seen	Last Seen	Hostname	IP	Port	Protocol	Status	TTL	Product	Version	Banner Information
GCHQ	Hacienda	Tue May 19 08:11:03 GMT 2009	Tue May 19 08:11:03 GMT 2009		[redacted]	80	tcp	filtered	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 08:11:03 GMT 2009	Tue May 19 08:11:03 GMT 2009		[redacted]	110	tcp	filtered	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 08:11:03 GMT 2009	Tue May 19 08:11:03 GMT 2009		[redacted]	111	tcp	filtered	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 08:11:03 GMT 2009	Tue May 19 08:11:03 GMT 2009		[redacted]	161	tcp	filtered	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 08:11:03 GMT 2009	Tue May 19 08:11:03 GMT 2009		[redacted]	162	tcp	filtered	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 08:11:03 GMT 2009	Tue May 19 08:11:03 GMT 2009		[redacted]	443	tcp	filtered	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 08:11:03 GMT 2009	Tue May 19 08:11:03 GMT 2009		[redacted]	500	tcp	filtered	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 08:07:29 GMT 2009	Tue May 19 08:07:29 GMT 2009		[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:15:01 GMT 2009	Tue May 19 04:15:01 GMT 2009		[redacted]	110	tcp	open	0	Kerio MailServer POP3 Server	6.1.2	4152.1242730171@kv_svr
GCHQ	Hacienda	Tue May 19 04:15:01 GMT 2009	Tue May 19 04:15:01 GMT 2009		[redacted]	443	tcp	open	0	Kerio MailServer Webmail	6.1.2	unknown
GCHQ	Hacienda	Tue May 19 04:15:01 GMT 2009	Tue May 19 04:15:01 GMT 2009		[redacted]	25	tcp	open	0	Microsoft ESMTP	6.0.3790.3959	unknown
GCHQ	Hacienda	Tue May 19 04:15:01 GMT 2009	Tue May 19 04:15:01 GMT 2009		[redacted]	80	tcp	open	0	Microsoft IIS webserver	6.0	unknown
GCHQ	Hacienda	Tue May 19 04:15:01 GMT 2009	Tue May 19 04:15:01 GMT 2009		[redacted]	21	tcp	open	0	Microsoft ftpd	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:15:01 GMT 2009	Tue May 19 04:15:01 GMT 2009		[redacted]	22	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:15:01 GMT 2009	Tue May 19 04:15:01 GMT 2009		[redacted]	23	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:15:01 GMT 2009	Tue May 19 04:15:01 GMT 2009		[redacted]	111	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:15:01 GMT 2009	Tue May 19 04:15:01 GMT 2009		[redacted]	161	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:15:01 GMT 2009	Tue May 19 04:15:01 GMT 2009		[redacted]	162	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:28 GMT 2009	Tue May 19 04:17:28 GMT 2009		[redacted]	21	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:28 GMT 2009	Tue May 19 04:17:28 GMT 2009		[redacted]	22	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:28 GMT 2009	Tue May 19 04:17:28 GMT 2009		[redacted]	23	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:28 GMT 2009	Tue May 19 04:17:28 GMT 2009		[redacted]	25	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:28 GMT 2009	Tue May 19 04:17:28 GMT 2009		[redacted]	80	tcp	open	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:28 GMT 2009	Tue May 19 04:17:28 GMT 2009		[redacted]	110	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:28 GMT 2009	Tue May 19 04:17:28 GMT 2009		[redacted]	111	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:28 GMT 2009	Tue May 19 04:17:28 GMT 2009		[redacted]	161	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:28 GMT 2009	Tue May 19 04:17:28 GMT 2009		[redacted]	162	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:28 GMT 2009	Tue May 19 04:17:28 GMT 2009		[redacted]	443	tcp	open	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:40 GMT 2009	Tue May 19 04:17:40 GMT 2009		[redacted]	21	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:40 GMT 2009	Tue May 19 04:17:40 GMT 2009		[redacted]	22	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:40 GMT 2009	Tue May 19 04:17:40 GMT 2009		[redacted]	23	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:40 GMT 2009	Tue May 19 04:17:40 GMT 2009		[redacted]	25	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:40 GMT 2009	Tue May 19 04:17:40 GMT 2009		[redacted]	80	tcp	open	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:40 GMT 2009	Tue May 19 04:17:40 GMT 2009		[redacted]	110	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:40 GMT 2009	Tue May 19 04:17:40 GMT 2009		[redacted]	111	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:40 GMT 2009	Tue May 19 04:17:40 GMT 2009		[redacted]	161	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:40 GMT 2009	Tue May 19 04:17:40 GMT 2009		[redacted]	162	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:40 GMT 2009	Tue May 19 04:17:40 GMT 2009		[redacted]	443	tcp	open	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:16:24 GMT 2009	Tue May 19 04:16:24 GMT 2009		[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue Jun 17 00:13:13 GMT 2008	Tue Jun 17 00:13:13 GMT 2008		[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue Jun 17 00:13:39 GMT 2008	Tue Jun 17 00:13:39 GMT 2008		[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue Jun 17 00:12:49 GMT 2008	Tue Jun 17 00:12:49 GMT 2008		[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue Jun 17 00:13:56 GMT 2008	Tue Jun 17 00:13:56 GMT 2008		[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue Jun 17 00:13:59 GMT 2008	Tue Jun 17 00:13:59 GMT 2008		[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue Jun 17 07:00:29 GMT 2008	Tue Jun 17 07:00:29 GMT 2008		[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue Jun 17 07:03:13 GMT 2008	Tue Jun 17 07:03:13 GMT 2008		[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue Jun 17 07:01:12 GMT 2008	Tue Jun 17 07:01:12 GMT 2008		[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue Jul 07 07:30:40 GMT 2009	Wed Feb 03 11:13:34 GMT 2010	80-247-147-40.reverse.nevakies.net	[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue Jul 07 07:32:20 GMT 2009	Wed Feb 03 11:14:55 GMT 2010	80-247-147-41.reverse.nevakies.net	[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue Jul 07 07:31:23 GMT 2009	Wed Feb 03 11:15:34 GMT 2010	80-247-147-42.reverse.nevakies.net	[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue Jul 07 07:32:13 GMT 2009	Wed Feb 03 11:13:39 GMT 2010	80-247-147-43.reverse.nevakies.net	[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue Jul 07 07:30:17 GMT 2009	Wed Feb 03 11:15:11 GMT 2010	80-247-147-44.reverse.nevakies.net	[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue Jul 07 07:32:54 GMT 2009	Wed Feb 03 11:13:15 GMT 2010	80-247-147-45.reverse.nevakies.net	[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue Jul 07 06:49:57 GMT 2009	Wed Feb 03 11:14:50 GMT 2010	80-247-147-46.reverse.nevakies.net	[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue Jul 07 06:47:17 GMT 2009	Wed Feb 03 11:14:09 GMT 2010	80-247-147-47.reverse.nevakies.net	[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue Jul 07 06:18:02 GMT 2009	Wed Feb 03 12:02:07 GMT 2010		[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue Jun 17 00:36:20 GMT 2008	Tue Jun 17 00:36:20 GMT 2008	ipo02-gw.emperion.net	[redacted]	23	tcp	open	0	Cisco router	unknown	unknown
GCHQ	Hacienda	Tue Jul 07 06:16:19 GMT 2009	Wed Feb 03 12:00:45 GMT 2010	ipo12-gw.emperion.net	[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown

- BUT, network analysis still manual!

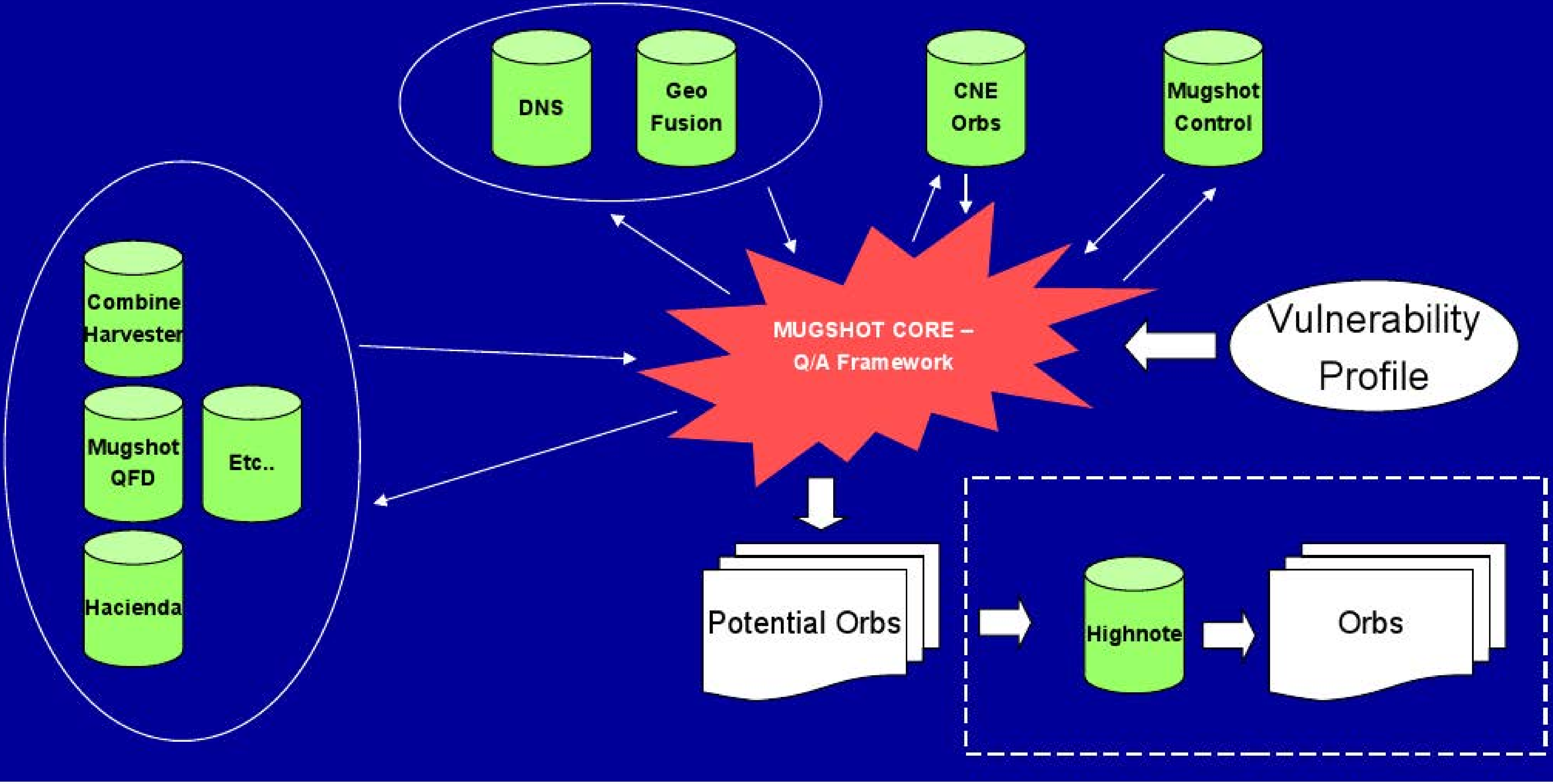
LANDMARK today...

- Network analysis tradecraft to determine vulnerable devices has been encoded within OLYMPIA

[redacted]

- [redacted] GSM provider
- NSA TAO requested assistance gaining access to the network
- Network analysis using OLYMPIA:
  - DNS query to determine IP address
  - IP address to network range
  - Network range to port scan
  - Are there any vulnerable devices in that range?
- Duration: < 5 minutes

Use Case 1: Finding Orbs



[redacted]

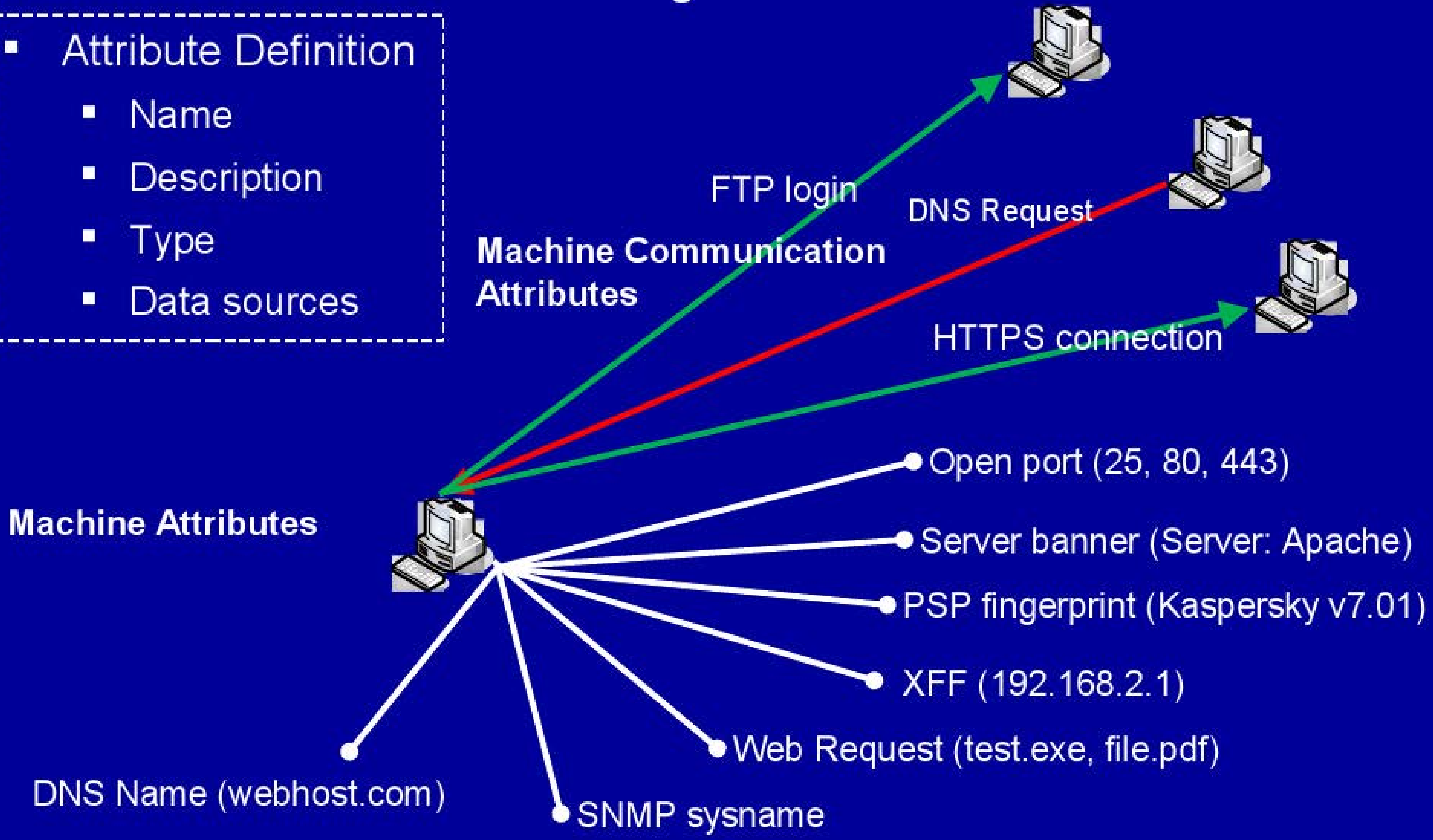
Benefits

- Automated Vulnerability Assessment
  - Using Vulnerability Profiles for Remote and Content Delivery vectors
- Automated Target Development and Monitoring
  - Identify and characterise target machines
- Profiles machines, including:
  - Browser, OS, PSP, Patch History
  - Activity
  - Download
- Automated Target Technology Tracking (Stats & Trends)
  - Browsers, OS, PSP etc
- ORB Identification
  - Initial ten fold increase in Orb Identification rate over manual process

[redacted]

Defining Attributes

- Attribute Definition
  - Name
  - Description
  - Type
  - Data sources



Machine Communication Attributes

FTP login

DNS Request

HTTPS connection

Machine Attributes

Open port (25, 80, 443)

Server banner (Server: Apache)

PSP fingerprint (Kaspersky v7.01)

XFF (192.168.2.1)

Web Request (test.exe, file.pdf)

DNS Name (webhost.com)

SNMP sysname

[redacted]

MUGSHOT GOALS

- Automated Target Characterisation and Monitoring
  - Automatically understand everything **important** about **CNE target networks** from passive and active sources.
- Automated Un-Targeted Characterisation
  - Automatically understand everything **important** about **all machines** on the Internet from passive and active sources.

GCHQ

[redacted]