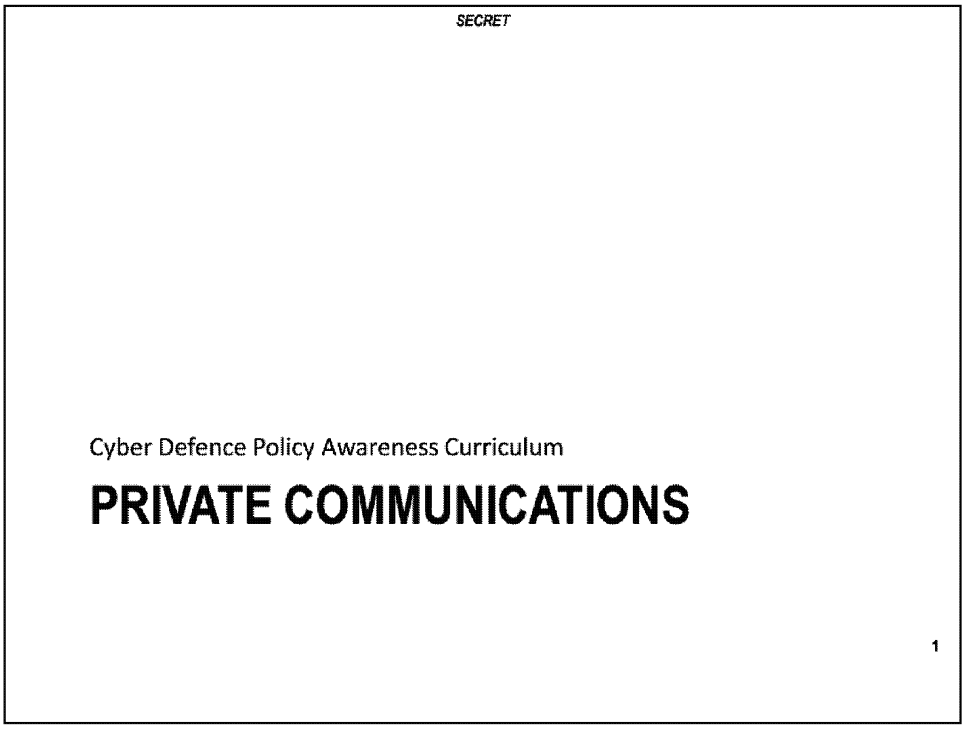
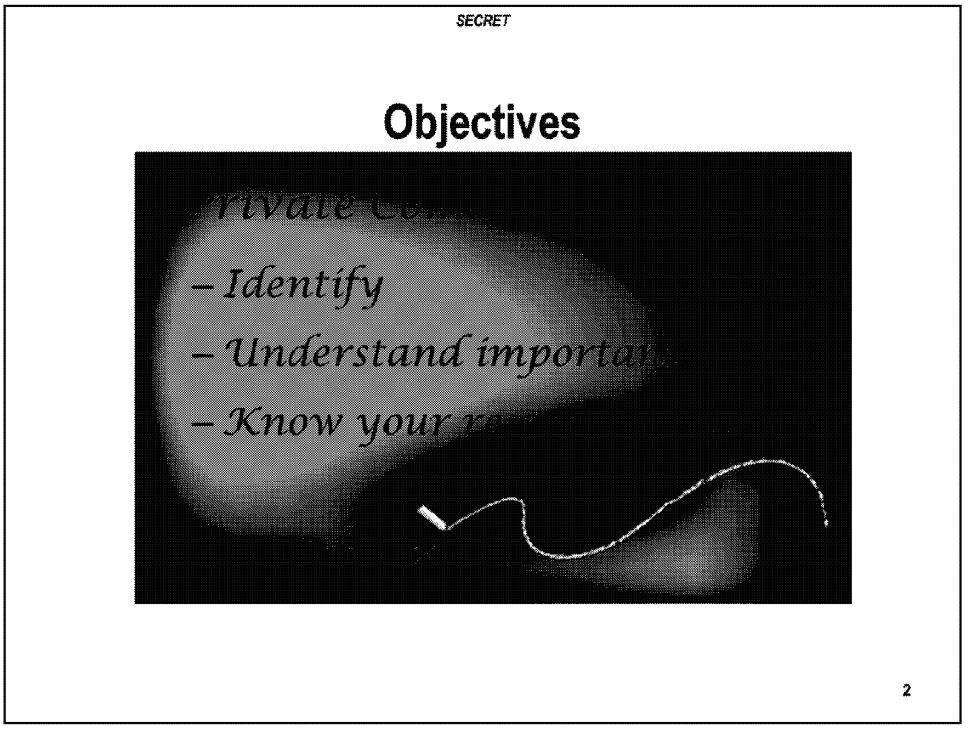


Rationale for this training covered on the “Objectives” slide.



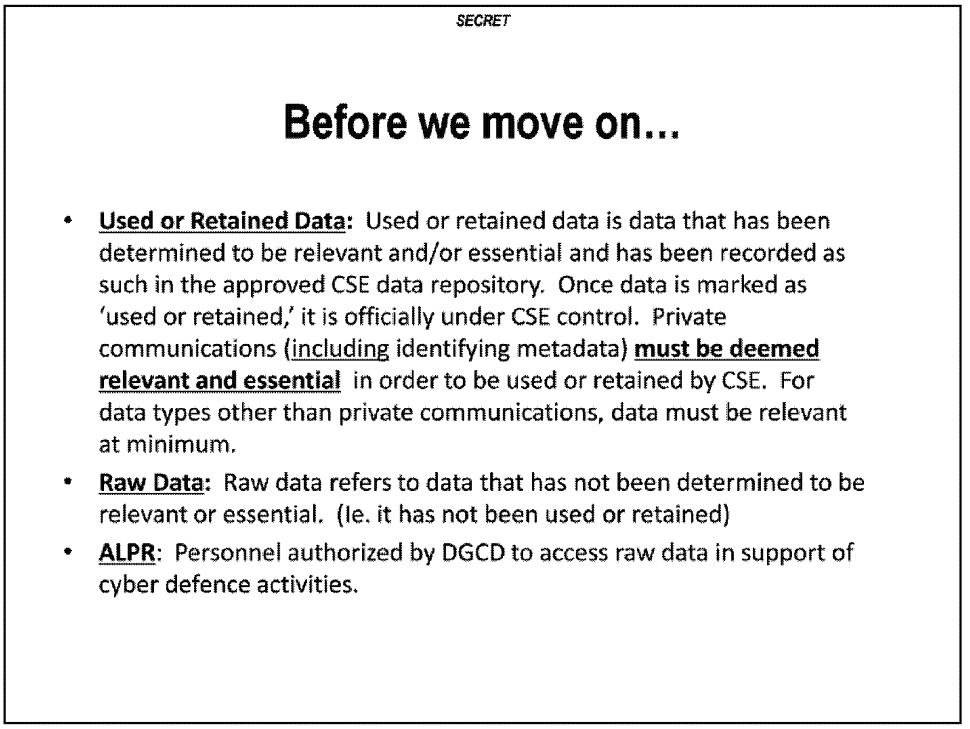
We want you to be able to **Identify Private Communications**, **understand** their importance from a Legal/Policy perspective and ultimately **enable** you to understand your responsibilities pertaining to working with Private Communications in the course of cyber defence activities.

-Essentially it comes down to a need to maintain the delicate balance between:

- 1) conducting the most advanced cyber defence operations that we can; and,
- 2) ensuring we are in-step with the stipulations of the law surrounding private communications.

- The goal of this workshop is to provide you with the knowledge you need to be able to confidently make decisions about what to do with private communications in various situations as you encounter it in your daily work and to appreciate how very important they are on so many levels!

- Our presentation includes an overview of how policy at CSE defines Private Communications, where our authority to intercept PCs originates – we will have more specific details on how you handle them in your daily work in our segment on Data Handling, but it should be clear, why PC requires your special attention.



Used or Retained Data:

Used or retained data is data that has been determined to be relevant and/or essential (as defined above) and has been recorded as such in the approved CSE data repository. Once data is marked as 'used or retained,' it is officially under CSE control. Private communications (including identifying metadata) **must be deemed relevant and essential** in order to be used or retained by CSE. For data types other than private communications, data must be relevant at minimum.

Raw Data: Raw data refers to data that has not been determined to be relevant or essential. (Ie. it has not been used or retained)

SECRET

What is a Private Communication?

According to OPS-1 (8.18)

A private communication is ....

"any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by an originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it, and includes any radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it".

4

Incidentally this OPS-1 definition is identical to the Criminal Code definition section 183.

AND

National Defence Act (Section 273.61) also points to the section 183 Criminal Code definition to confirm the same definition for CSE's purposes.

Let's look at it in 'non-legal' jargon.....

What is a Private Communication?

A Private Communication (PC) is:

- An oral communication or telecommunication intercepted [redacted]

Where:
- An expectation of privacy is reasonable;
- Is human to human; and,
- The originator is in Canada; or,
- The originator intends the recipient to be in Canada.

5

Our **OPS** definition is derived from the Criminal Code section 183. The National Defence Act (273.61) further references the Criminal Code) definition of Private Communication for CSE Purposes.

With our work covering [redacted] of GC networks … we are going to be dealing with one end Canadian PCs!!

NOTE: Unlike SIGINT – the concern here is not Canadian **Citizenship** – We don't look at people – We look at the threat. For our purposes, a PC is one end 'in CANADA or expected to be IN CANADA'.

Discuss [redacted]

The decision has been to **not debate if a communication is** [redacted]

Basically regardless of whether the content of the communication has not yet reached the intended recipient(s), **ITS operators will treat the communication as a Private Communication**…

Where:

- An expectation of privacy is reasonable; and,
- The originator is in Canada
- The originator intends the recipient to be in Canada

Why are we concerned about PC?

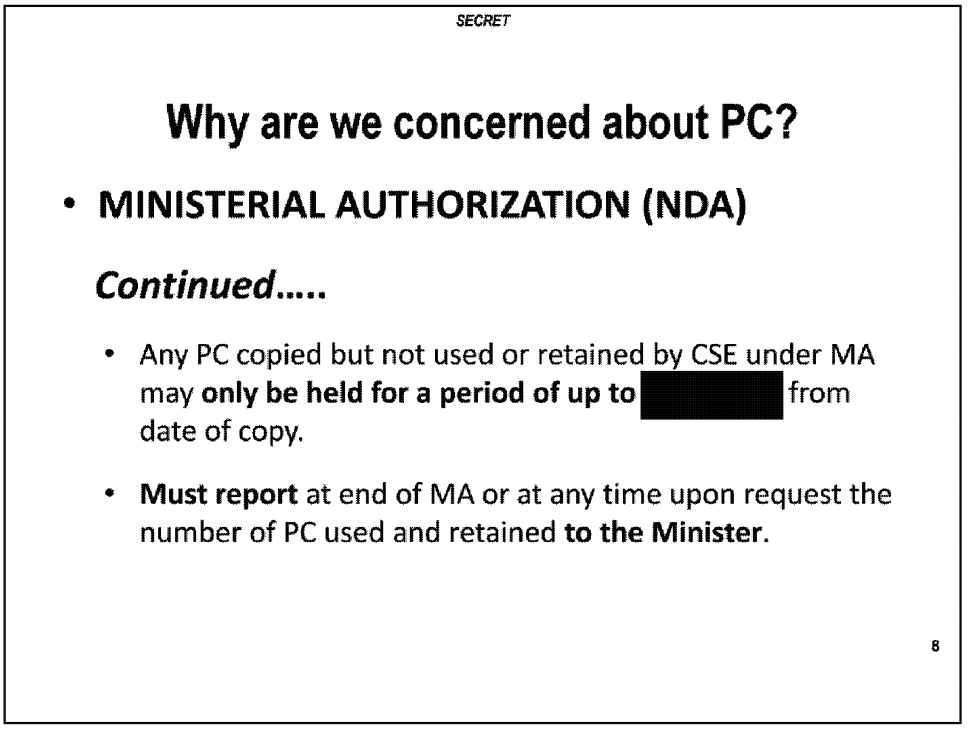
MINISTERIAL AUTHORIZATION (NDA)

The Minister outlines conditions that **MUST** be satisfied to intercept PC

- Intercept **to the extent necessary** to identify, isolate or prevent harm to GC
- To use or retain **PC - MUST** be **ESSENTIAL** to identify, isolate or prevent harm of CG systems/networks.
- Subject to measures to **protect privacy of Canadians** – at minimum follow OPS 1 & Ops 1-14

7

Ministerial Authorization- NDA Sec 273.65 (3) – **CSE** – can intercept under MA for the **SOLE purpose** of **protecting** the **computer systems or networks of the Government of Canada** (**Note – NOT systems of importance…it's not applicable for the entire mandate B description)



So when you have to identify your PC's in [redacted]….please remember…this is important for many reasons…the Minister even wants to know how many we keep!

Private Communications

And so naturally….

- Very serious **and** important factor in Cyber Defence Activities as we strive to operate:
  - Lawfully
  - In accordance with Ministerial Authorization
  - In accordance with Ministerial Directives

9

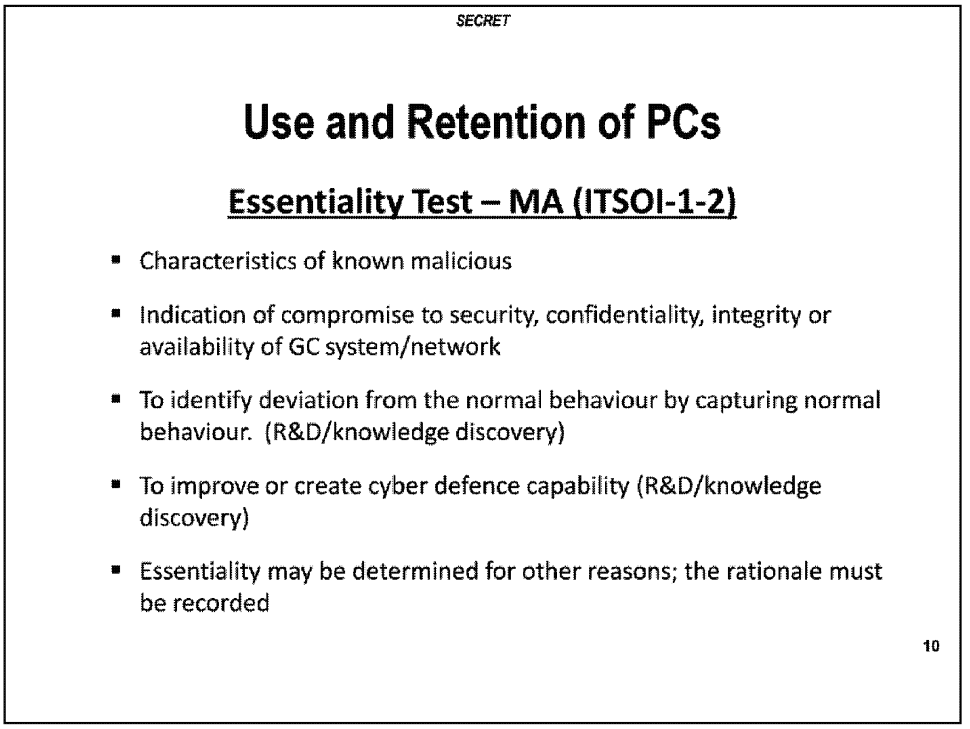
-**Financial Administration Act** (can intercept for specific reasons)

-**Criminal Code of Canada** (can intercept for specific reasons)

-**Privacy Act** (must protect privacy!)

-**National Defence Act** Subject to measures to protect the privacy of Canadians

- **NDA – Ministerial Authorization** –can be issued that allows for interception of PC **ONLY if**:
  -necessary to identify, isolate or prevent harm to GC computer systems or networks;
  -could not reasonably be obtained by other means
  -consent of persons whose private communications may be intercepted cannot reasonably be obtained.
  -satisfactory measures are in place to ensure that only information that is essential to identify, isolate or prevent harm to the GC systems or networks will be used and retained
  -satisfactory measures are in place to protect the privacy of Canadians in the use or retention of that information
- **Ministerial Authorization –** Minister can impose additional conditions – for us :
  - PC copied but not 'used and retained' – must be deleted within [redacted]
  - Report to the Minister on number of PCs used and retained (essential) to identify, isolate or prevent harm to the GC systems or networks.



OPS-1, sec.4.9 Essentiality – Private Communications in MA Operations: A private communication may only be used or retained if essential to identify, isolate or prevent harm to GC computer systems or networks. Such information must be tracked in order to allow CSEC to fulfill Ministerial reporting requirements concerning use and retention.

ITSOI-1-2: The Essentiality test: Private communications obtained during cyber defence activities under MA may only be used or retained if **essential to identify, isolate or prevent harm** to GC computer systems or networks.

Private communications obtained under MA may be essential if they:

- have one or more significant characteristics similar to malicious activities of concern previously seen in cyber defence activities;
- provide an indication that a computer system is or may be attempting to, or succeeding in affecting the confidentiality,

  integrity, and/or availability of GC computer systems or networks;
- characterize the normal behaviour of a computer system or network, or a part of it, for the purpose of identifying deviation

  from this normal behaviour which could be indicative of possible malicious activity against GC computer systems or networks;
- can be used to improve or create a cyber defence capability.

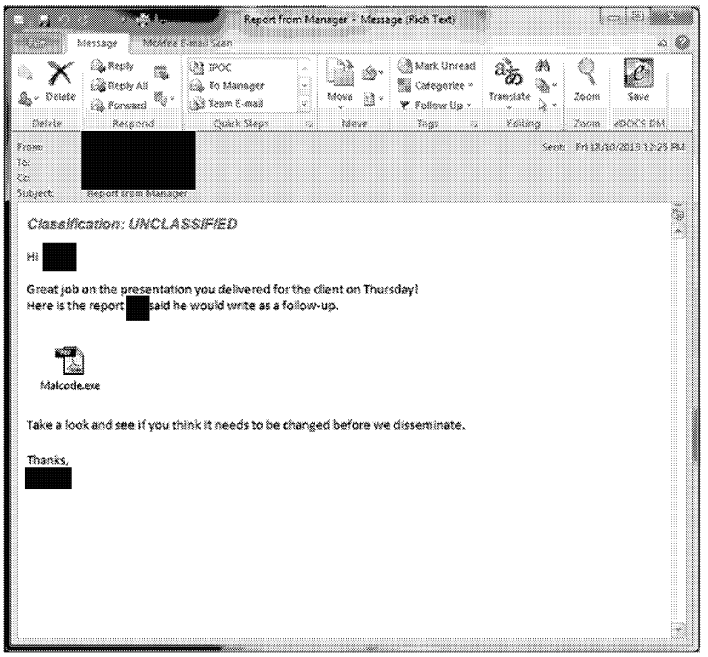
Essentiality may be determined for other reasons; the rationale must be recorded.

Use and Retention of PCs

Essentiality Test – DPSO (Non-MA)

IRRELEVANT

SECRET

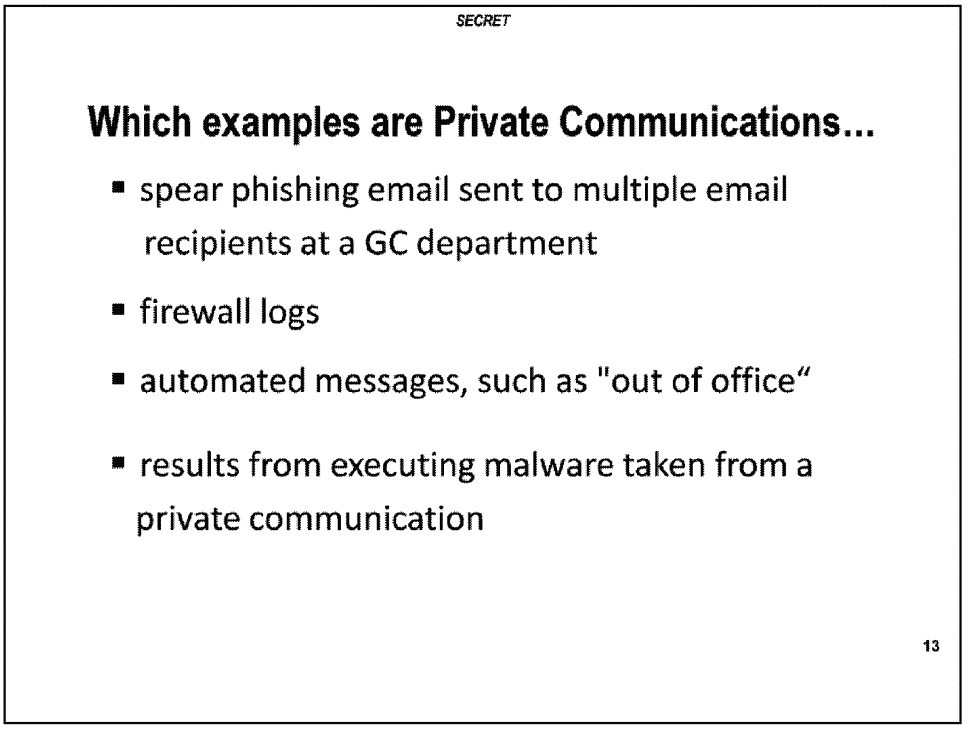


12

Example to demonstrate a problem that attachments could possibly pose:

In this example, the sender and recipient are using GC emails, so the communication is a PC.

Despite that the file -- an executable masking as a .pdf – seems harmless but contains malcode, this attachment **IS still considered a PC.** (It is part of the communication)

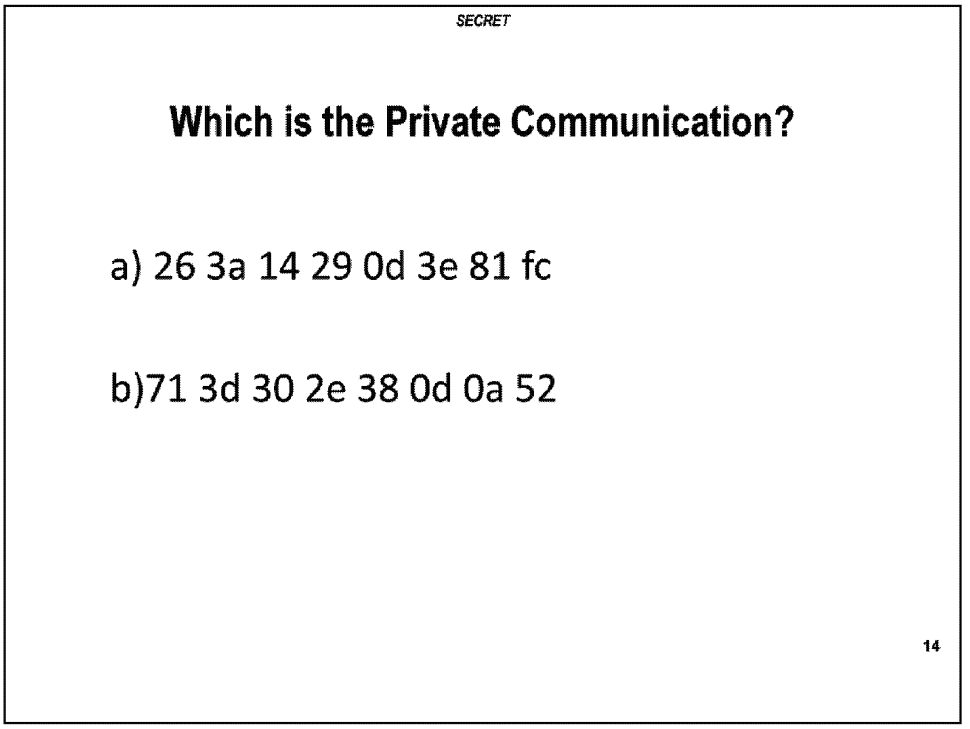


Spear phising – **YES**

Firewall logs – **NO**

Automated messages such as 'out of office' - **NO** - counts as machine generated- the machine has no expectation of privacy. A private communication must have a human originator and a human recipient. This applies even if the automatic message contains extracts from the original message, such as a subject line.

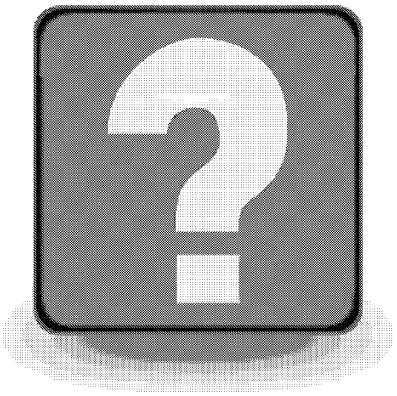
Results from executing malware – **NO** (it is derivative information and not considered PC)



First one – payload data (malicious code), delivered as an email attachment (we have recipient consent!!!)

Second – foreign to foreign.

SECRET



15